# Connecticut CVO Credentialing System

*Release 1.0*

user

**manual**

*prepared for*

**State of Connecticut**
**CVISN/PRISM Steering Committee**

*prepared by*

**Cambridge Systematics, Inc.**

*January 2004*

www.camsys.com

*user manual*

# Connecticut CVO Credentialing System

*Release 1.0*

*prepared for*

State of Connecticut
CVISN / PRISM Steering Committee

*prepared by*

Cambridge Systematics, Inc.
100 CambridgePark Drive, Suite 400
Cambridge, Massachusetts  02140

*January 2004*

# Table of Contents

# List of Tables

# List of Figures

# List of Figures
## (continued)

# 1.0 System Overview and Structure

Connecticut's CVO Credentialing System is the State's single point of access for motor carriers and service bureaus wishing to conduct the following activities:

- On-line IRP transactions (specific transactions are provided by the IRP system; refer to the IRP system documentation for more information);
- On-line IFTA transactions:
  - Request a new IFTA license (new carriers only),
  - Renew an existing IFTA license,
  - Request additional IFTA decals, and
  - Link to the New York Regional Processing Center (RPC) to file IFTA quarterly taxes;
- On-line OS/OW transactions (specific transactions are provided by the OS/OW system; refer to the OS/OW system documentation for more information) – scheduled for delivery in April 2004; and
- View carrier and vehicle information on-line.

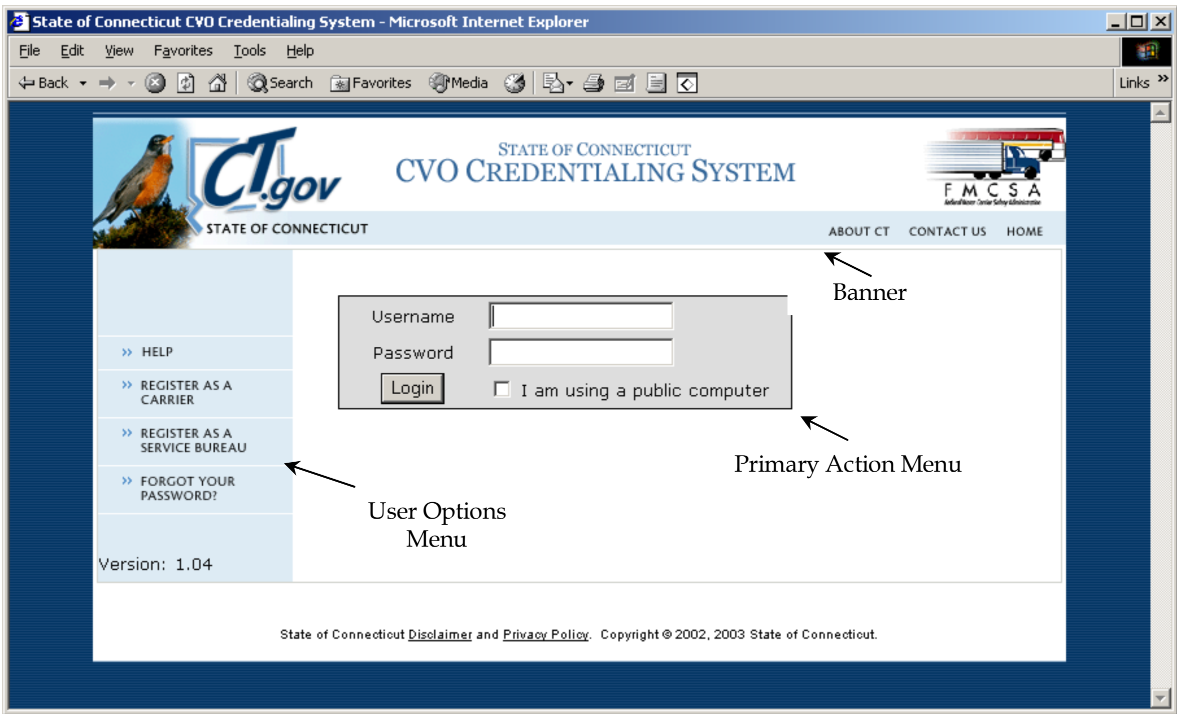
The production CVO Credentialing System generally is available 24 hours a day via the Internet at https://www.cvisn.state.ct.us/ct/. Motor carriers must have an Internet browser (Internet Explorer, Netscape, etc.), Internet access, and an e-mail account to access Connecticut's CVO Credentialing System. The CVO Credentialing System is a secure site that requires a username and password.

The content of the CVO Credentialing System is dynamically displayed based on the user's privileges and location within the system. The structure of the Credentialing System remains constant throughout. A banner containing a series of links (State of Connecticut home page, Federal CVISN page, Contact Us information, etc.) appears at the top of the CVO Credentialing System. A user options menu appears on the left-hand side of the screen – the options vary depending on the user's access rights and where he/she is in the system. The primary action menu is located in the middle of the screen and provides a series of links to the main actions (View carrier and vehicle information, Apply for IFTA transactions, etc.) that the user can access through the CVO Credentialing System.

Clicking "Help" on the user options menu on any page in the CVO Credentialing System will open a separate browser window displaying help information. The Help information is tailored to the page from which it is selected.

Figure 1.1 illustrates standard features of the CVO Credentialing System.

**Figure 1.1 CVO Credentialing System Standard Features**




## ■ 1.1 Screen Reference

Details regarding each page of the CVO Credential System can be found in Appendix A. This information is drawn from the Connecticut CVISN/PRISM CI/CVIEW Detailed (Physical) Design, which was finalized in November 2003.

# 2.0 Setting Up a CVO Credentialing System Account

A user must register to use the CVO Credentialing System the first time they visit the site. Motor carriers wishing to register should click the "Register as a Motor Carrier" link in the user options menu of the login screen. Service bureaus wishing to register should click the "Register as a Service Bureau" link in the user options menu of the login screen.

The registration processes for both motor carriers and service bureaus are described below.

## 2.1 Registering as a Motor Carrier

A motor carrier user registering with the CVO Credentialing System will be required to enter the following information:

- **Username –** A unique name between six and 20 characters long for the carrier's Credentialing System account;
- **Password –** An alphanumeric string between six and 20 characters in length (underscore, period, and hyphen may be included in the password);
- **Password Confirmation –** Retyped password to ensure that the password was entered correctly;
- **E-mail Address –** The e-mail address to which a forgotten password should be sent;
- **Company Name –** The legal company name for the motor carrier;
- **Tax ID Number –** The motor carrier's FEIN or SSN;
- **Business Address –** The physical location of the motor carrier; and
- **Phone Number –** The contact phone number for the motor carrier.

If available, a motor carrier also should enter:

- U.S. DOT Number;
- IRP Account Number;
- IFTA Account Number;
- Tax Registration Number; and
- Doing Business As (DBA) name.

By default, the system assumes that a carrier's Mailing Address and Contact Address are the same as its Business Address. To modify the Mailing Address and/or Contact Address, the user should uncheck the appropriate box at the bottom of the form and enter the required information.

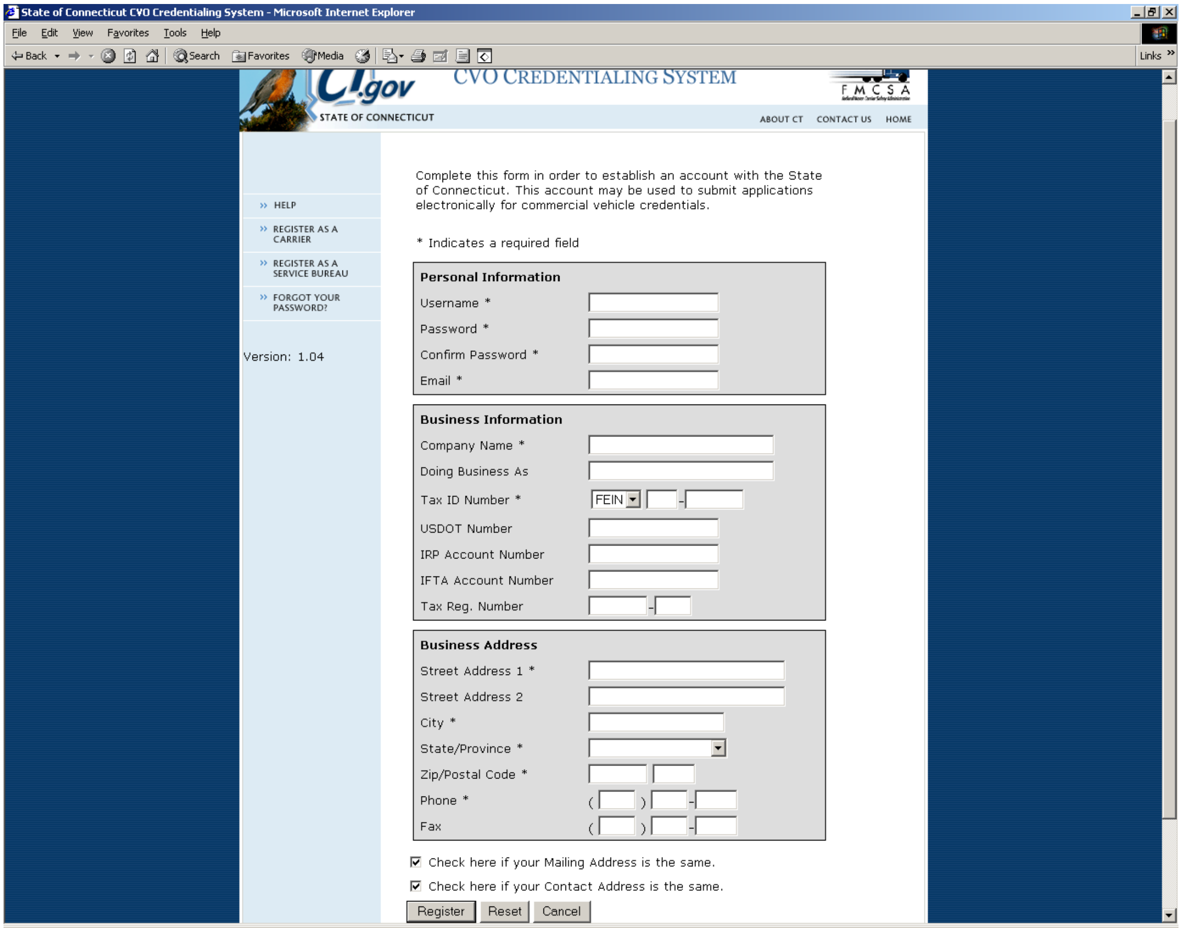
Three buttons can be found at the bottom of the screen:

- **Register –** Completes the registration process;
- **Reset –** Clears the form without completing the registration process; and
- **Cancel –** Returns the user to the initial log-in screen without completing the registration process.

Once the Carrier Registration Form is complete, the user should click the "Register" button to submit the information. The data entry page has built-in validation to ensure that the user enters information in the correct format (e.g., only numeric characters can be entered in the phone number field). If an error is detected, an error message will be displayed in a red box at the top of the screen. The user must correct the specified error and reenter his/her password before pressing the "Register" button to re-submit the registration.

Figure 2.1 illustrates the Registration form for a Motor Carrier.

**Figure 2.1 Form to Register as a Motor Carrier**




## ■ 2.2 Registering as a Service Bureau

A service bureau wishing to set-up an account to use the CVO Credentialing System must enter the following information:

- **Username –** A unique name between six and 20 characters long for the service bureau's Credentialing System account;
- **Password –** An alphanumeric string between six and 20 characters in length (underscore, period, and hyphen may be included in the password);
- **Password Confirmation –** Retyped password to ensure that the password was entered correctly;

- **E-mail Address –** The e-mail address to which a forgotten password should be sent;
- **Company Name –** The legal company name of the service bureau;
- **Business Address –** The physical location of the service bureau; and
- **Phone Number –** The contact phone number for the service bureau.

A service bureau also can enter the following information:

- Doing Business As (DBA) name; and
- Tax ID Number.

By default, the system assumes that a service bureau's Mailing Address and Contact Address are the same as its Business Address. To modify the Mailing Address and/or Contact Address, the user should uncheck the appropriate box at the bottom of the form and enter the required information

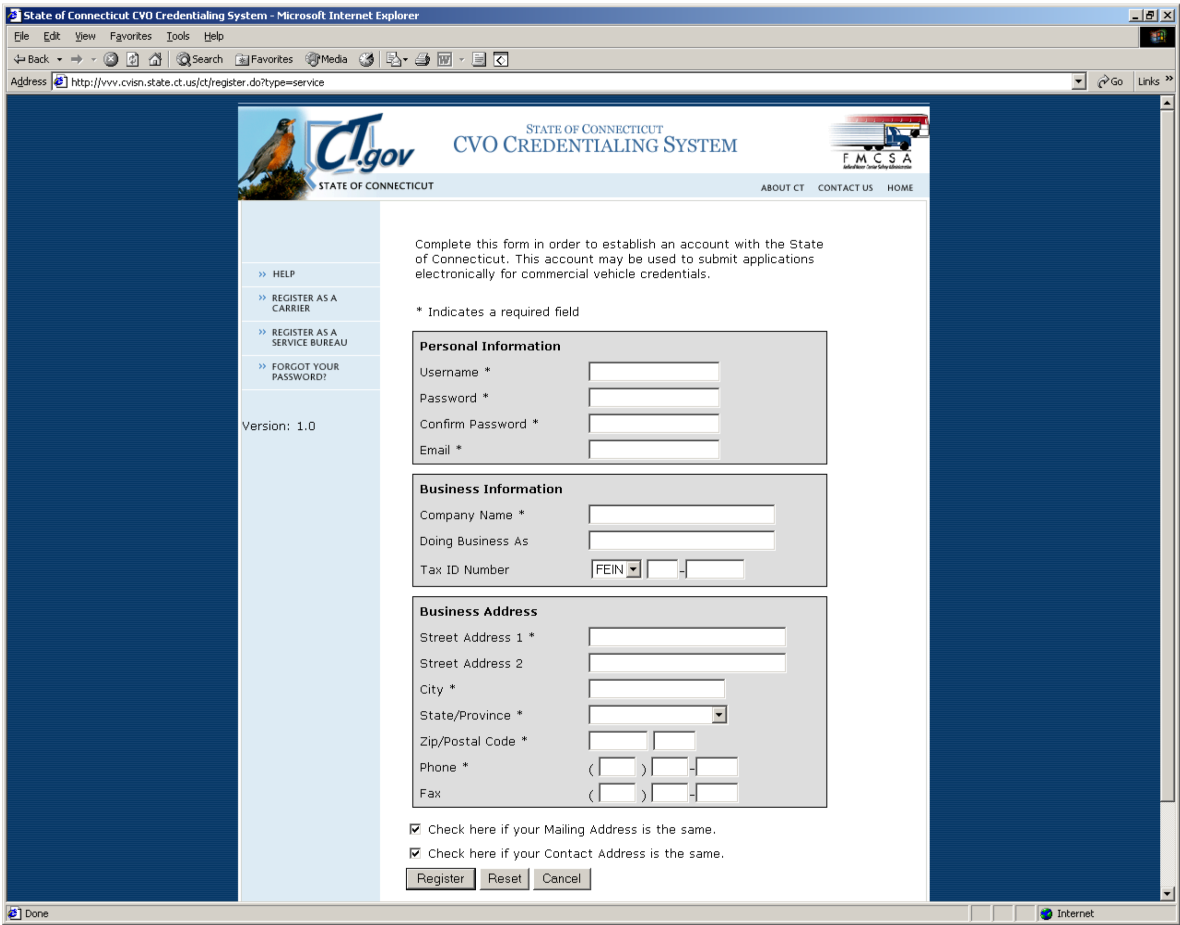
Three buttons can be found at the bottom of the screen:

- **Register –** Completes the registration process;
- **Reset –** Clears the form without completing the registration process; and
- **Cancel –** Returns the user to the initial log-in screen without completing the registration process.

Once the Service Bureau Registration Form is complete, the user should click the "Register" button to submit the information. The data entry page has built-in validation to ensure that the user enters information in the correct format (e.g., only numeric characters can be entered in the phone number field). If an error is detected, an error message will be displayed in a red box at the top of the screen. The user must correct the specified error and reenter his/her password before pressing the "Register" button to re-submit the registration.

Figure 2.2 illustrates the Registration form for a Service Bureau.

### Figure 2.2 Form to Register as a Service Bureau




## ■ 2.3 State Users

The CVO Credentialing System also supports State users. There is no self-registration process for a State user. In order to create a State user account, the State's designated representative should contact Cambridge Systematics (CS) and request that the account be created. The State's representative must supply the following information for a State user:

- **User's Name –** The name of the State user;
- **E-mail Address –** The e-mail address of the State user; and
- **Agency –** The agency of the State user.

The State's representative also may supply the following information:

- Physical address for the user, if different from the main agency address; and
- Contact phone number for the user.

CS will create the State user account within one business day and supply the username and password directly to the State user.

## 2.4 User Privileges

The following privileges exist for all CVO Credentialing System accounts:

- **Enabled –** All accounts are enabled by default.
- **Master Account –** Accounts created through self-registration are master accounts. Sub-accounts are created from within a master account and are discussed in Section 6.0.
- **Maintain Account –** By default, master accounts can maintain their own information. Master accounts can maintain all the information associated with the master account, including addresses and identifiers like FEIN/SSN, which exist at the business level as well as contact information associated with the master account. Sub-accounts can maintain only information that is unique to the sub-account, e.g., contact information, if the master grants this privilege to the sub-account. This option is not enabled for State users.
- **Maintain Sub-accounts –** By default, master accounts can create, maintain, and enable/disable sub-accounts associated with the master account. Sub-accounts may not maintain other sub-accounts. This option is not enabled for State users.
- **View Carrier and Vehicle Information –** By default, carriers and service bureaus are prevented from viewing snapshot information. Access to view snapshot information must be granted explicitly by the State upon agreement from all CVISN/PRISM agencies. Carriers may be granted access to view their own carrier and vehicle snapshots. Service bureaus will not be granted access to view snapshots. This option may be granted to sub-accounts by the master account. This option is enabled for State users, who have the ability to view snapshots for any carrier.

- **Access IFTA –** By default, the Department of Revenue Services will allow access to the $\text{IFTA}_{\text{CS}}$ credential web application by newly registered users. This option may be granted to sub-accounts by the master account. This option is not enabled for State users.

- **Access IRP –** By default, the Department of Motor Vehicles will not allow access to the MVS Express web application. Access must be granted explicitly by DMV personnel, who also must supply a valid MVS Express account name associated with the carrier or service bureau. This option may be granted to sub-accounts by the master account. This option is not enabled for State users.

- **Access OS/OW –** By default, the Department of Transportation will allow access to the e-PASS web application. This option may be granted to sub-accounts by the master account. This option is not enabled for State users.

- **Access RPC –** By default, the Department of Revenue Services will allow access to the New York Regional Processing Center's tax filing web application by newly registered users. This option may be granted to sub-accounts by the master account. This option is not enabled for State users.

# 3.0 Accessing CVO Credentialing System

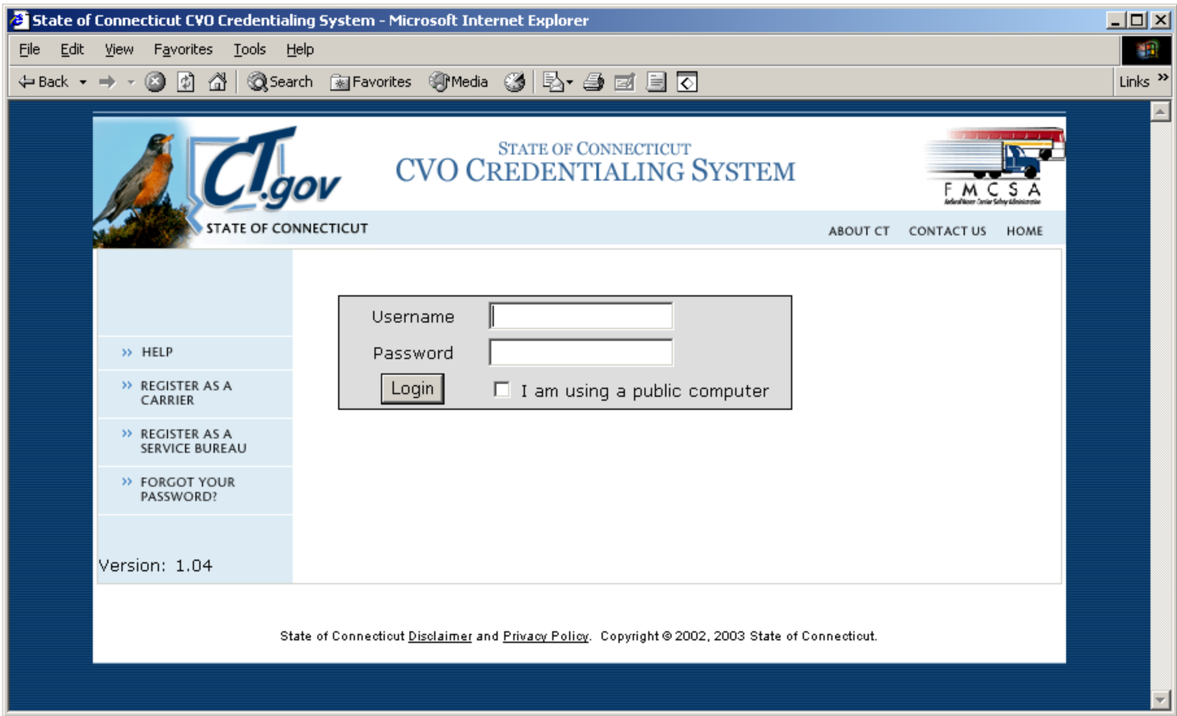
Registered users must enter their username and password and click the "Login" button to access the CVO Credentialing System. If an inaccurate username or password is entered, an error message will be displayed in a red box at the top of the screen. The user will be prompted to re-enter his/her username and password.

The user should click the "I am using a public computer" box if he/she is accessing the system from a public computer (library, Internet kiosk, etc.). This option provides a higher level of security by logging the user off the system after 10 minutes of inactivity. If this box is not checked, the system will log the user off after four hours of inactivity. Timeout values may be different for CVO Credential subsystems, such as the IFTA tax filing application supplied by the RPC.

If the user forgets his/her password, it can be reset by clicking "Forgot Your Password?" in the user options menu. The user will be prompted to enter his/her username. A system-generated password will be sent to the e-mail address associated with the CVO Credentialing System Account (entered during registration). The user will be required to use this new password to access the system. The system-generated password can be changed for motor carriers and service bureaus by using the "Edit My Account" function. State users can contact the CVO Credentialing System helpdesk for assistance in resetting passwords. Helpdesk information is available on the Contact Us page.

Figure 3.1 illustrates the CVO Credentialing System Login Page.

# Figure 3.1 CVO Credentialing System Login Page



# 4.0 CVO Credentialing System Main Menu

The main page of the CVO Credentialing System dynamically displays the links for actions that the user is authorized to perform. The default privileges for the master account (set-up during registration) are determined by the State. The master account holder can create sub-accounts (with separate usernames and password) for employees. Master account holders also can limit the functions that can be accessed by their sub-accounts (i.e., allow IRP staff to access only the CVO Credentialing System's IRP functionality).

The following options can be selected via the user options menu:

- **Edit My Account –** Enables the user to edit the information entered during registration or sub-account creation;
- **Manage User Accounts –** Allows the user to add, edit, and enable/disable sub-accounts that have been set-up under the user's master account; and
- **Logout –** Allows the user to exit/log out of the system.

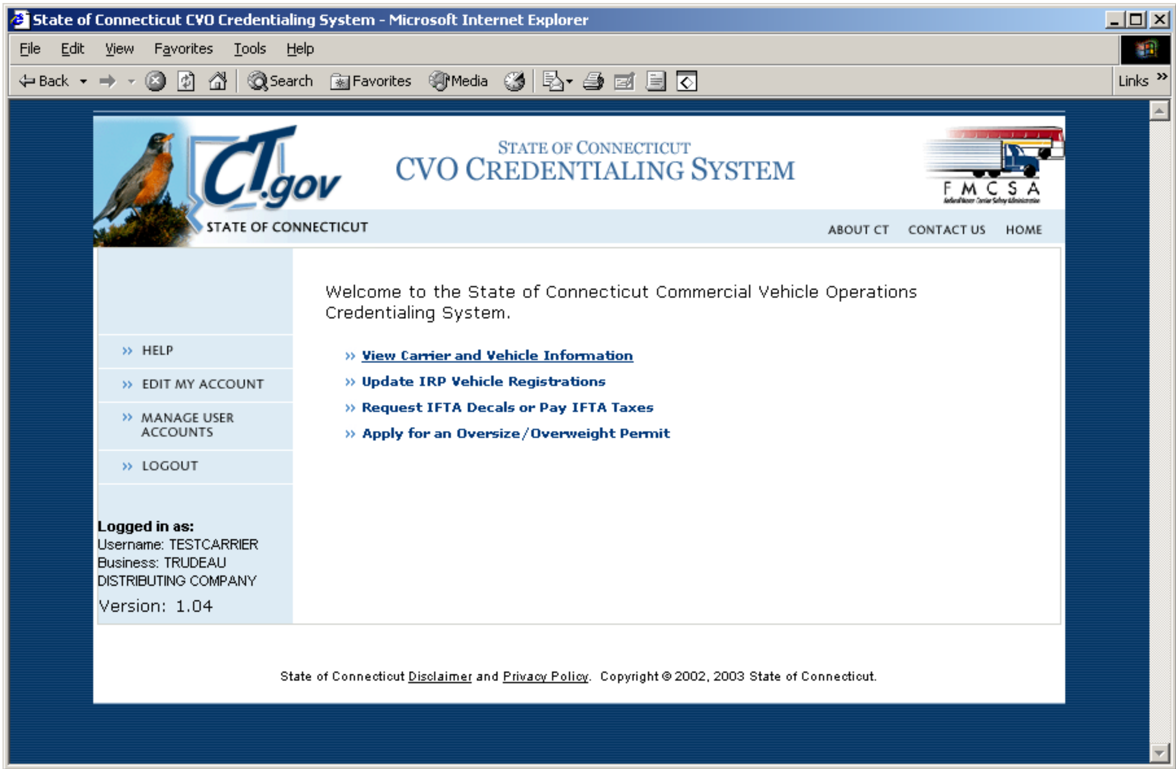
Access to help is available from the user options menu. Clicking the "Help" link will open a new window displaying help information relevant to the current page. Not all options listed in the help window can be performed by all users.

The following options can be selected via the main menu:

- View Carrier and Vehicle Information;
- Update IRP Vehicle Registration;
- Request IFTA Decals or Pay IFTA Taxes; and
- Apply for an Oversize/Overweight Permit (scheduled for April 2004).

Figure 4.1 illustrates the CVO Credentialing System Main Menu.

# Figure 4.1 CVO Credentialing System Main Menu



# 5.0 Editing User Account

Selecting the "Edit My Account" link will display a form that enables the user to edit the information entered during registration. All fields except username and FEIN/SSN can be updated. Figure 5.1 illustrates the form.

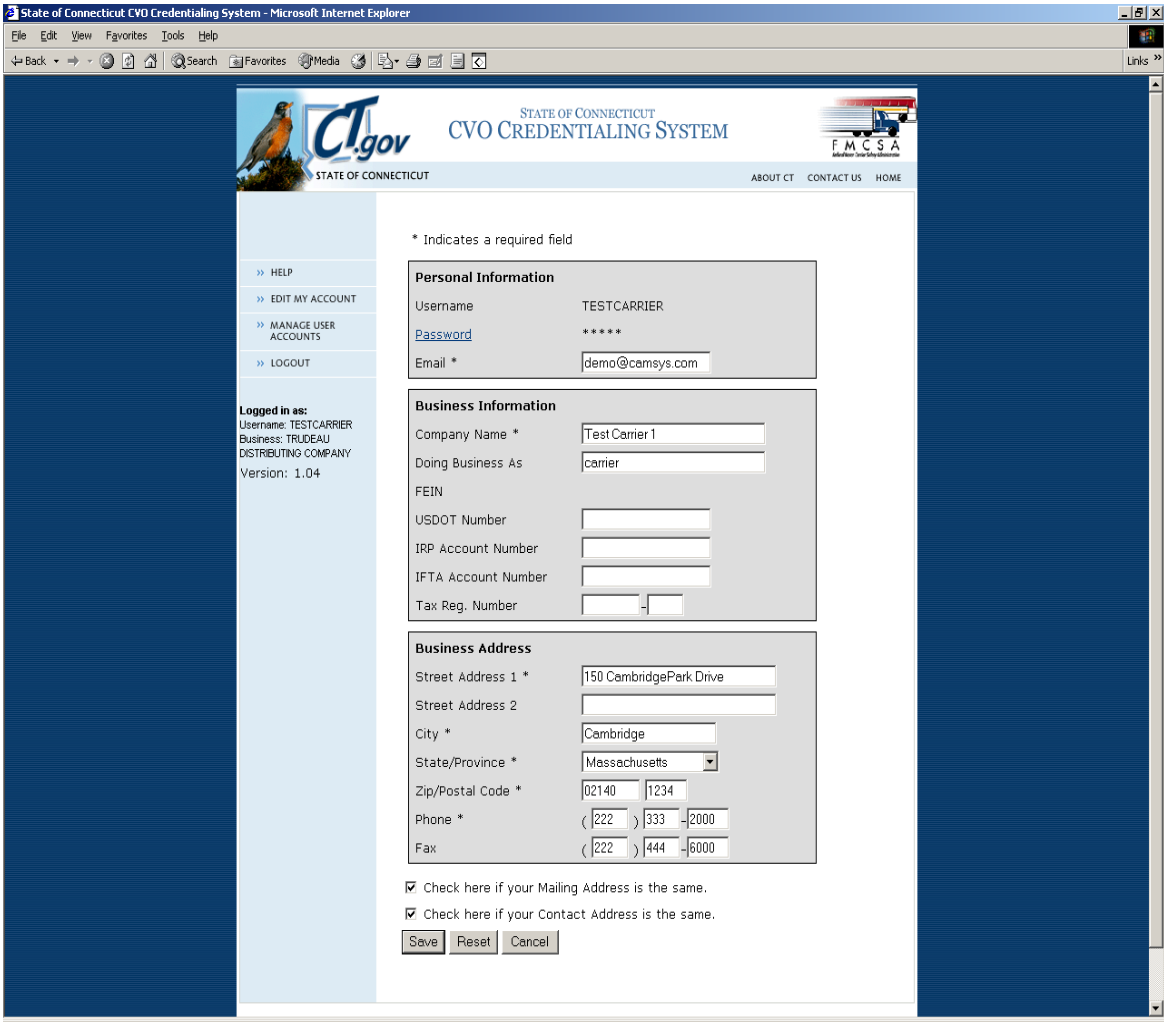
Three buttons can be found at the bottom of the screen:

- **Save –** Returns the user to the main menu after saving the changes;
- **Reset –** Restores original entries to the form without saving the changes; and
- **Cancel –** Returns the user to the main menu without saving the changes.

Once the necessary information has been updated, the user should click the "Save" button at the bottom of the form. The system will verify that all required fields have been completed and validate the information, as necessary. If an error is detected, an error message will be displayed in a red box at the top of the screen. The user must correct the specified error before pressing the "Save" button to re-submit the changes.

Figure 5.1 illustrates the Maintain Account page.

## Figure 5.1 Form to Edit User Account




# ■ 5.1 Changing Passwords

Selecting the "Password" link will open a separate window where the user may change their password. The user must enter their current password, provide a new password and confirm the new password.

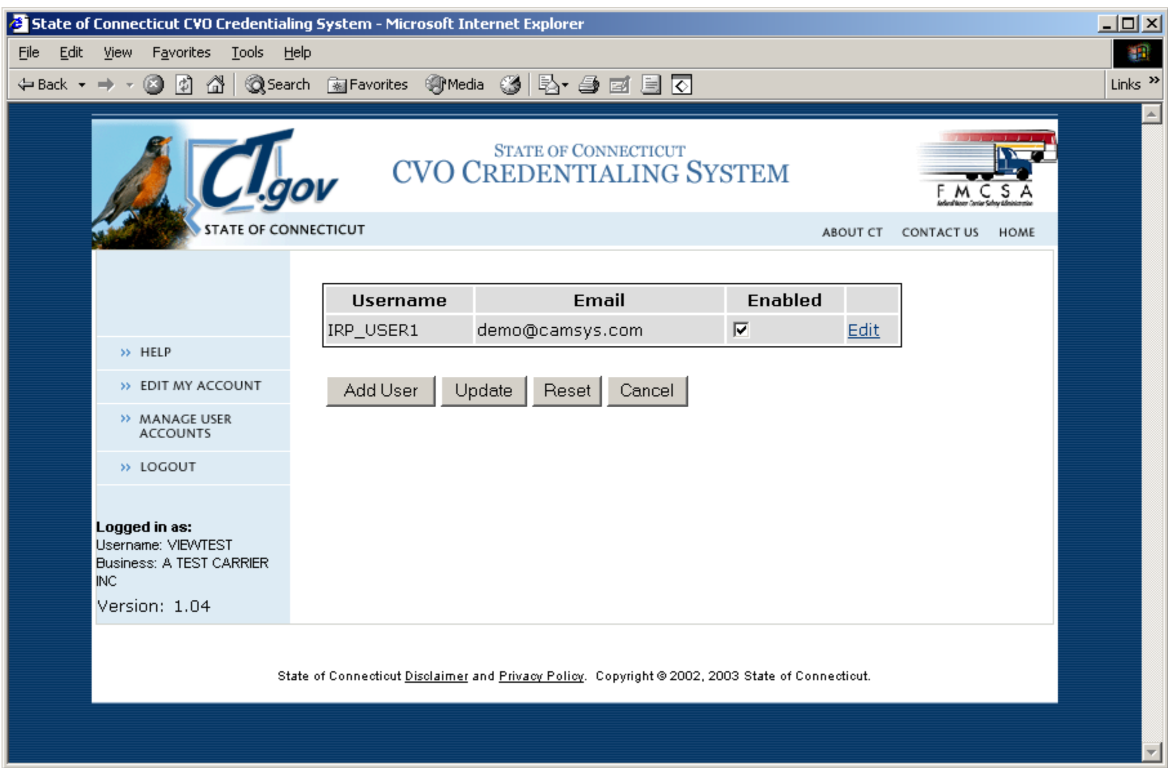
Two buttons can be found at the bottom of the screen:

- **Change –** Verifies that the values entered are correct, updates the password, and returns the user to Maintain Account page; and
- **Cancel –** Returns the user to the Maintain Account page without changing the password.

# 6.0 Managing Subaccounts

"Manage User Accounts" allows an authorized user to add, edit, and enable/disable subaccounts that have been set-up under the carrier's master account. The user should click the "Manage User Accounts" link to manage his/her subaccounts. A summary of current subaccounts will be displayed, as shown in Figure 6.1.

**Figure 6.1 Summary of User's Subaccounts**




## 6.1 Creating Subaccounts

To add a new subaccount, the user should click the "Add User" button.

The user will be required to enter the following information:

- Unique username (between six and 20 characters long);
- Password (alpha-numeric and between six and 20 characters long); and
- E-mail address for the subaccount.

The Business and Mailing Addresses for the subaccount always will match that of the master account. The system assumes that contact address is the same as the business address. If this is not the case, users should uncheck the box at the bottom of the form and enter the required contact information.

The user also can select the functions that the subaccount will be able to perform:

- IFTA Access – IFTA license transactions;
- IFTA Quarterly Access – IFTA quarterly tax filings;
- IRP Access – IRP transactions;
- OSOW Access – OS/OW transactions (scheduled for April 2004);
- Edit Profile – Maintain subaccount information; and
- View Carrier – Carrier and Vehicle Information.

A subaccount user will only see links for the functions that they are authorized to perform. The master account may only grant to a subaccount those functions that are accessible to the master account. For example, if the master account has not been authorized to submit IRP applications, then the IRP Access privilege will not appear on this page and cannot be authorized for a subaccount.

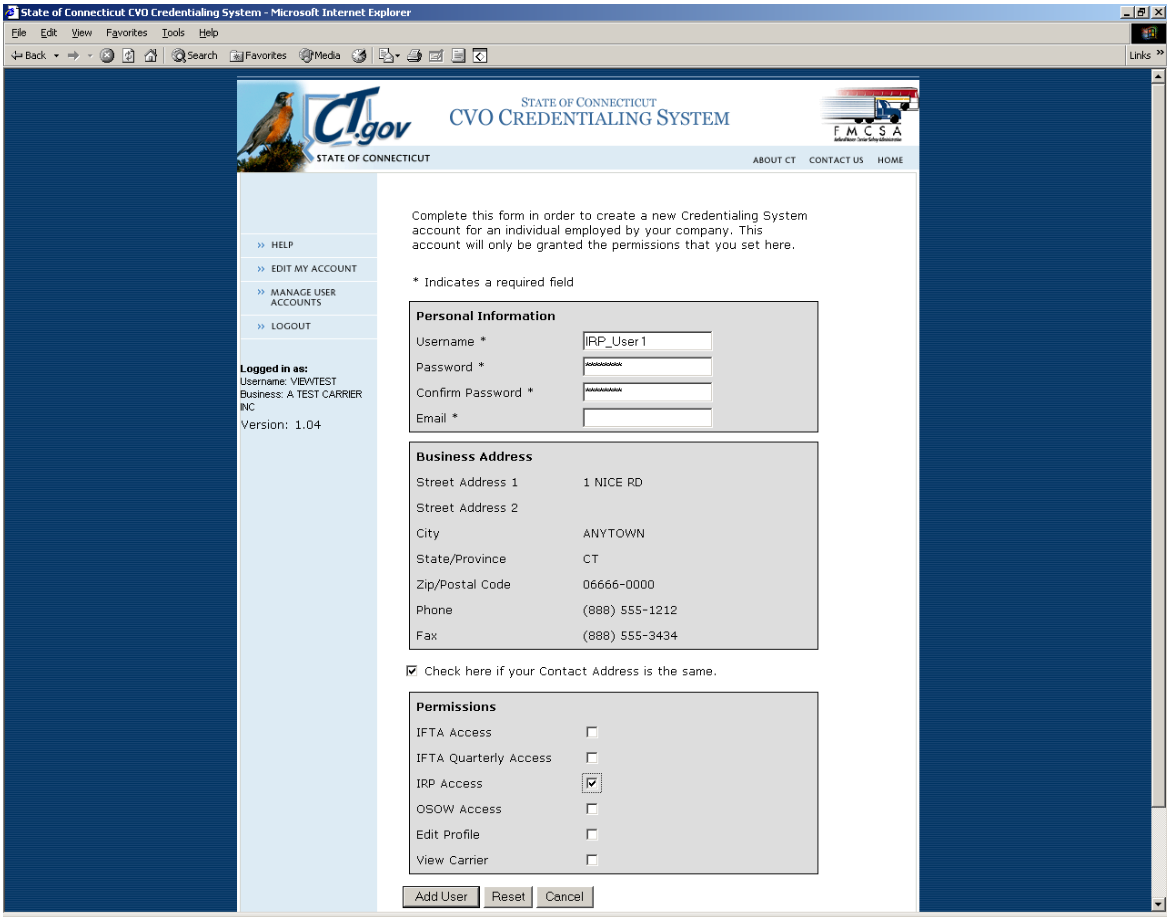
Three buttons can be found at the bottom of the screen:

- **Add User –** Returns the user to the summary of subaccounts after saving the information;
- **Reset –** Restores original entries to the form without saving the changes; and
- **Cancel –** Returns the user to the summary of subaccounts without saving the information.

Once the data entry form is completed, the user should click the "Add User" button.

The data entry page has built-in validation to ensure that the user enters information in the correct format (e.g., only numeric characters can be entered in the phone number field). If an error occurs, an error message will be displayed in a red box at the top of the screen. The user must correct this error, enter the password, and re-type the password before pressing the "Add User" button again. Figure 6.2 illustrates the form to create a subaccount.

## Figure 6.2 Subaccount Creation




# ■ 6.2 Editing Subaccounts

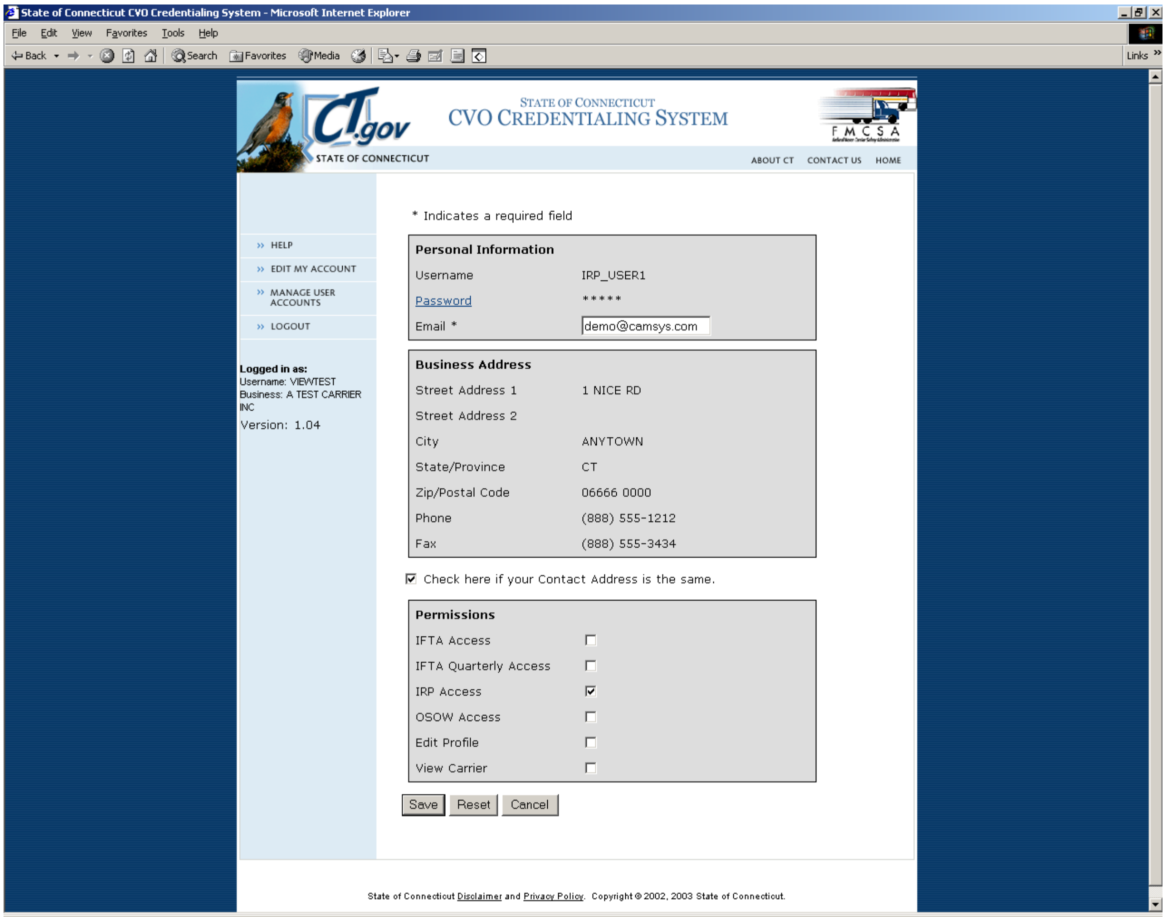
A master account holder can edit subaccount information by clicking the "Edit" link on the subaccount line on the summary page. All fields, except the subaccount's username and business address, can be edited. Changing a subaccount's password will open a separate window.

Three buttons can be found at the bottom of the screen:

- **Save –** Returns the user to the main page after saving the changes;
- **Reset –** Restores original entries to the form without saving the changes; and
- **Cancel –** Returns the user to the main menu page without saving the changes.

Once the subaccount has been updated, the user should click the "Save" button. Figure 6.3 illustrates the form for editing a subaccount.

**Figure 6.3 Form to Edit a Subaccount**

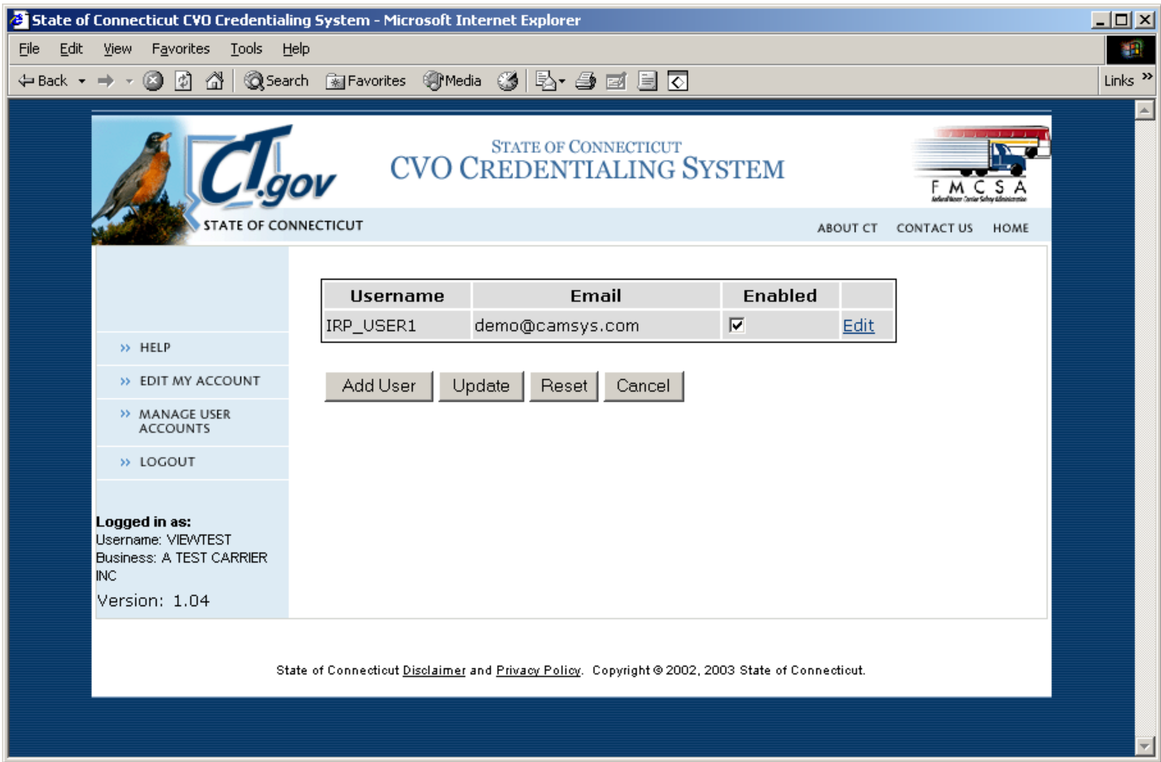



## 6.3 Enabling/Disabling Subaccounts

A subaccount can be disabled by the master account holder. To disable a subaccount, the user should uncheck the box in the "Enabled" column on the subaccount line on the summary page. A subaccount can be reactivated, by checking the box in the "Enabled" column. Clicking the "Update" button saves the changes.

Figure 6.4 illustrates the form used to enable/disable subaccounts.

## Figure 6.4 Enabling/Disabling Subaccounts



# 7.0 Viewing Carrier and Vehicle Information

Clicking the "View Carrier and Vehicle Information" link from the main menu will display a Carrier Selection Page when logged in as a service bureau or State user. The Carrier Selection Page is illustrated in Figure 7.1.

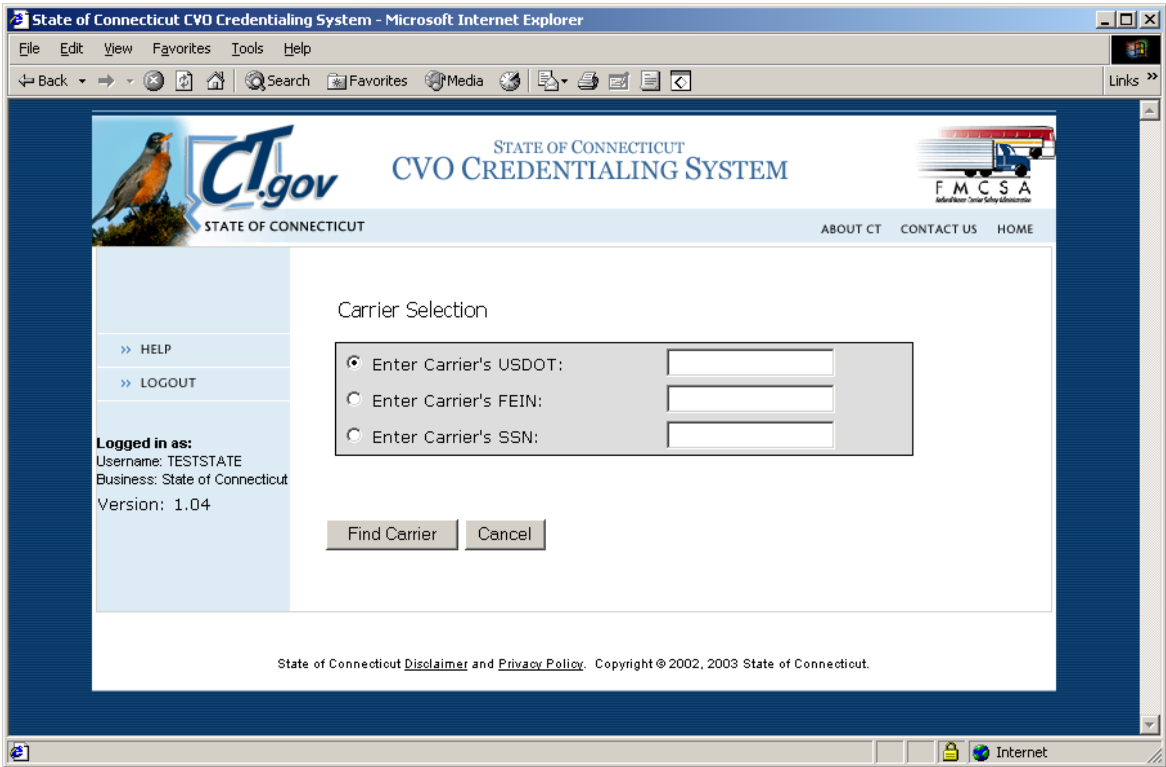
A service bureau or State user may query for a carrier's data using the following identifiers:

- U.S. DOT Number;
- FEIN; and
- SSN.

Only one identifier may be selected at a time.

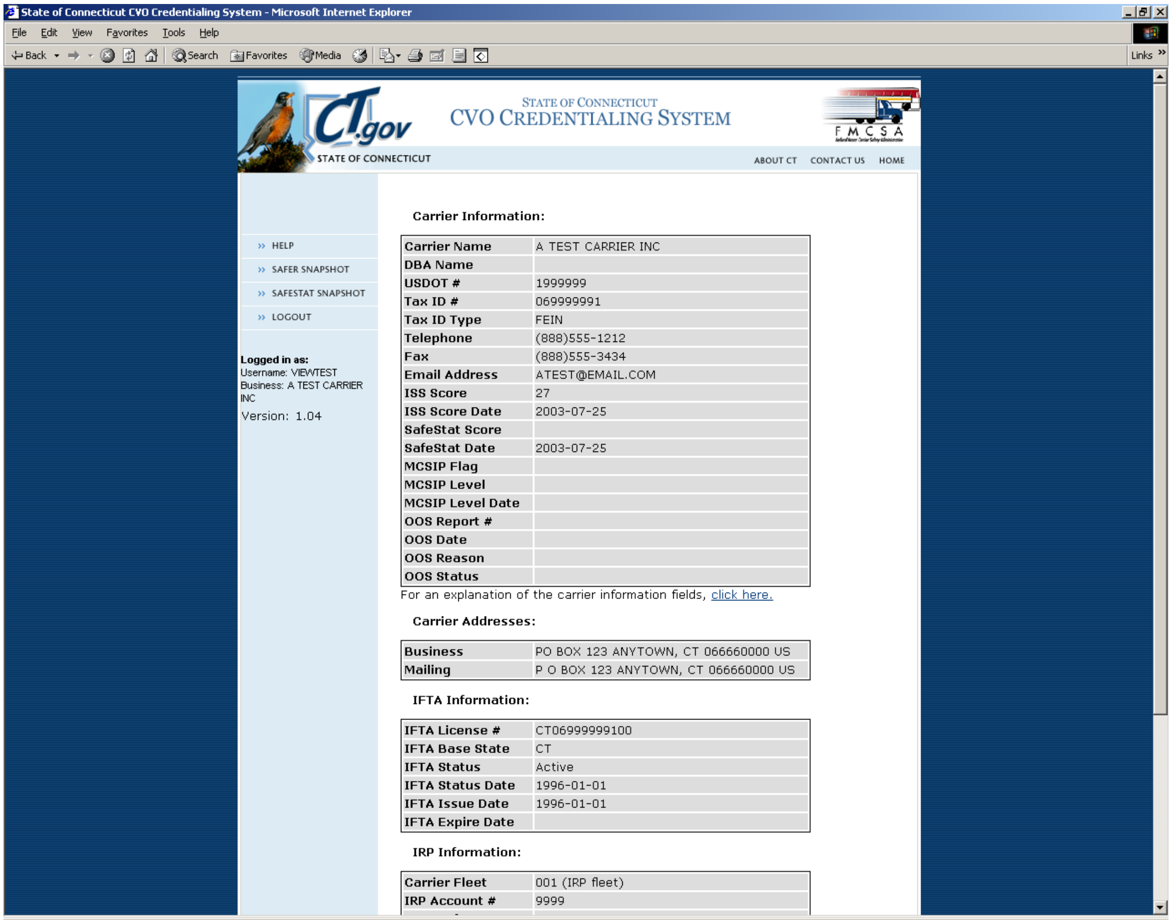
The user should enter a single carrier identifier in the appropriate field and click the "Find Carrier" button. All available information for that carrier will be displayed. If no information is available for the carrier, the message "Carrier is not found. Please try again." will be displayed at the top of the Carrier Selection Page. The user can attempt to query for the carrier's information using one of the other search criteria. The user also may click the "Cancel" button to return to the main menu.

## Figure 7.1 Carrier Selection Page




For a motor carrier, clicking the "View Carrier and Vehicle Information" link from the main menu will display a summary of the safety and credential data associated with the carrier as shown in Figure 7.2. The user will only be allowed to see his/her company's information. A sub-account user will only be allowed to see this information if he/she has been given the necessary access by the master account holder.

## Figure 7.2 Carrier and Vehicle Snapshot

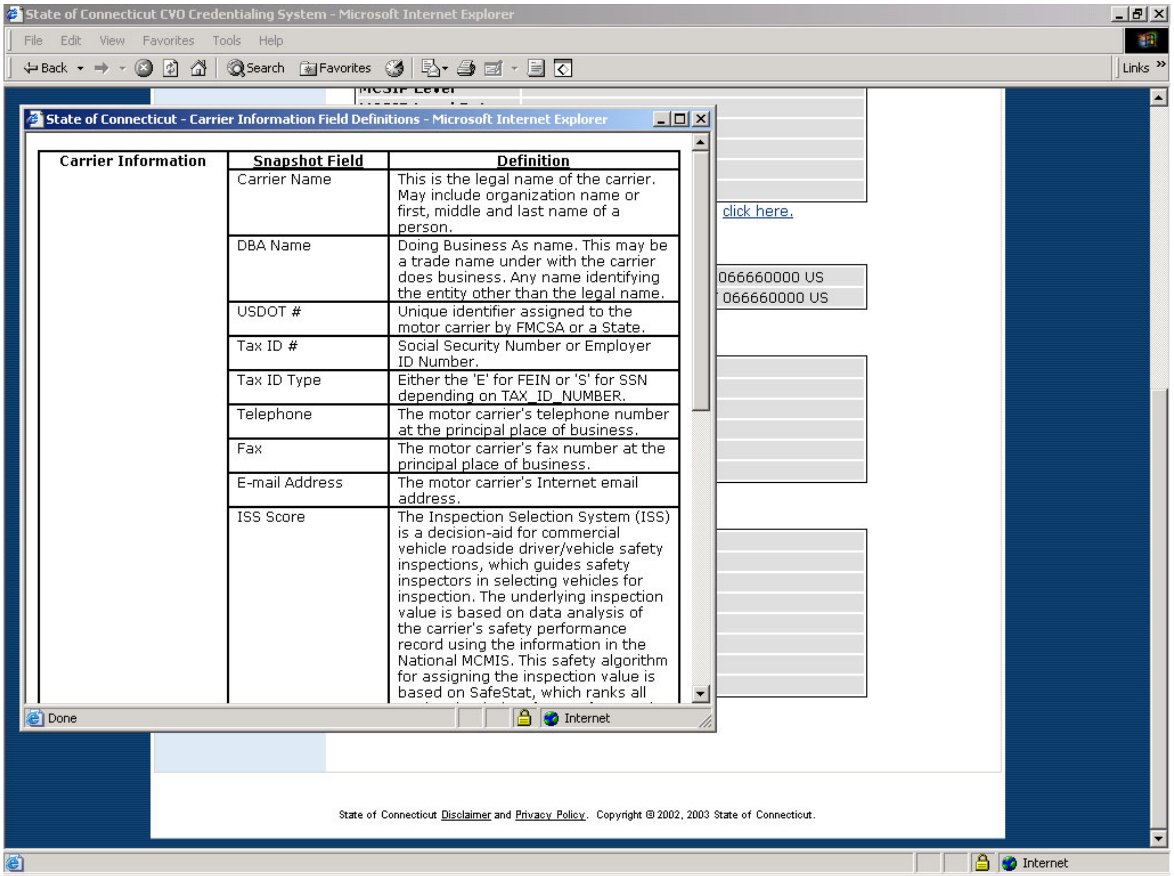



The Carrier information includes:

- **Name –** Carrier and DBA names;
- **Identifiers–** U.S. DOT, Tax ID number, and Tax ID Type;
- **Contact Information –** Telephone number, Fax number, E-mail address;
- **Federal Safety Scores –** ISS, SAFESTAT, MCSIP, OOS information;
- **Addresses –** Carrier physical and mailing addresses;
- **IFTA Information –** License information, base state, current status, issue and expiration dates; and
- **IRP Information –** Fleet information, account number, registration state, current status, issue and expiration dates, comments.

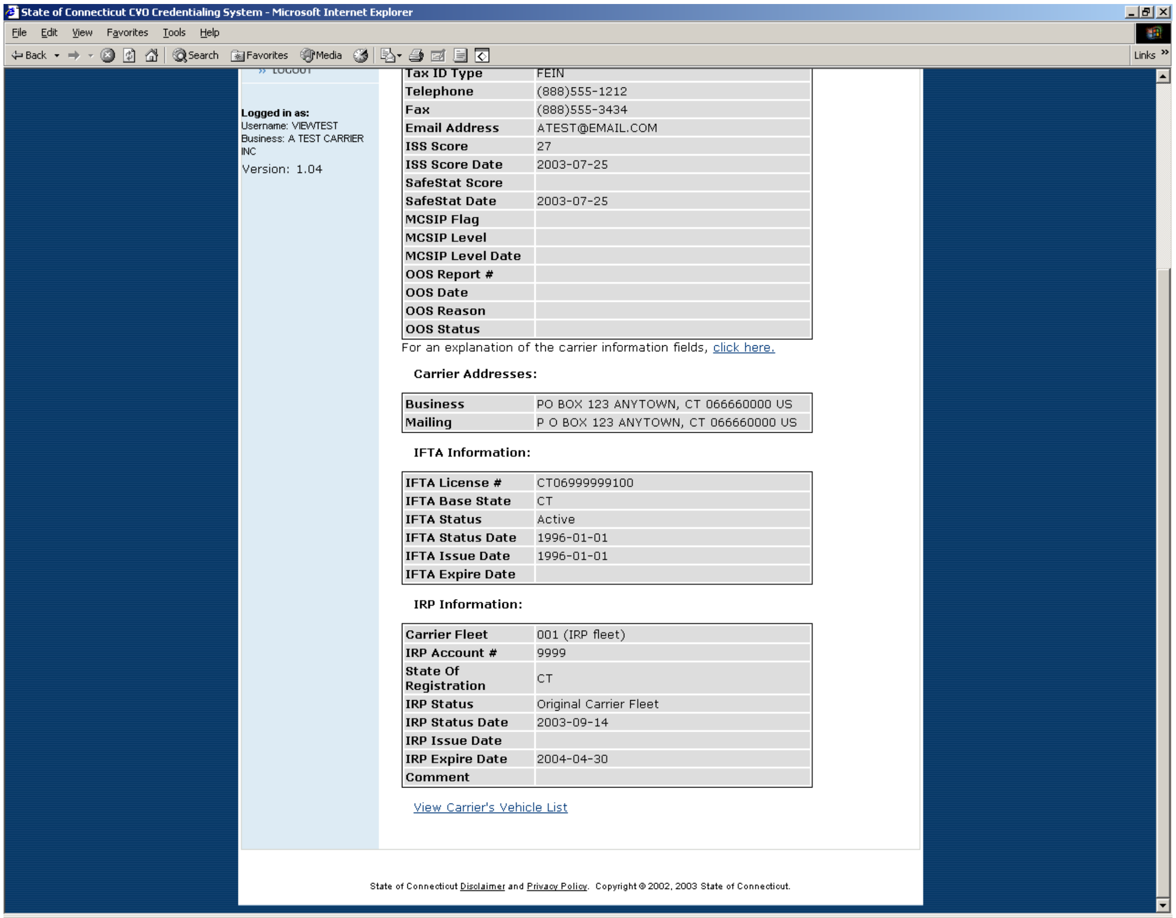
A link to information explaining the carrier fields is present on the carrier information screen as shown in Figure 7.2. Clicking the "click here" link will show definitions of the various carrier information fields as shown in Figure 7.3.

## Figure 7.3 Carrier Field Definitions



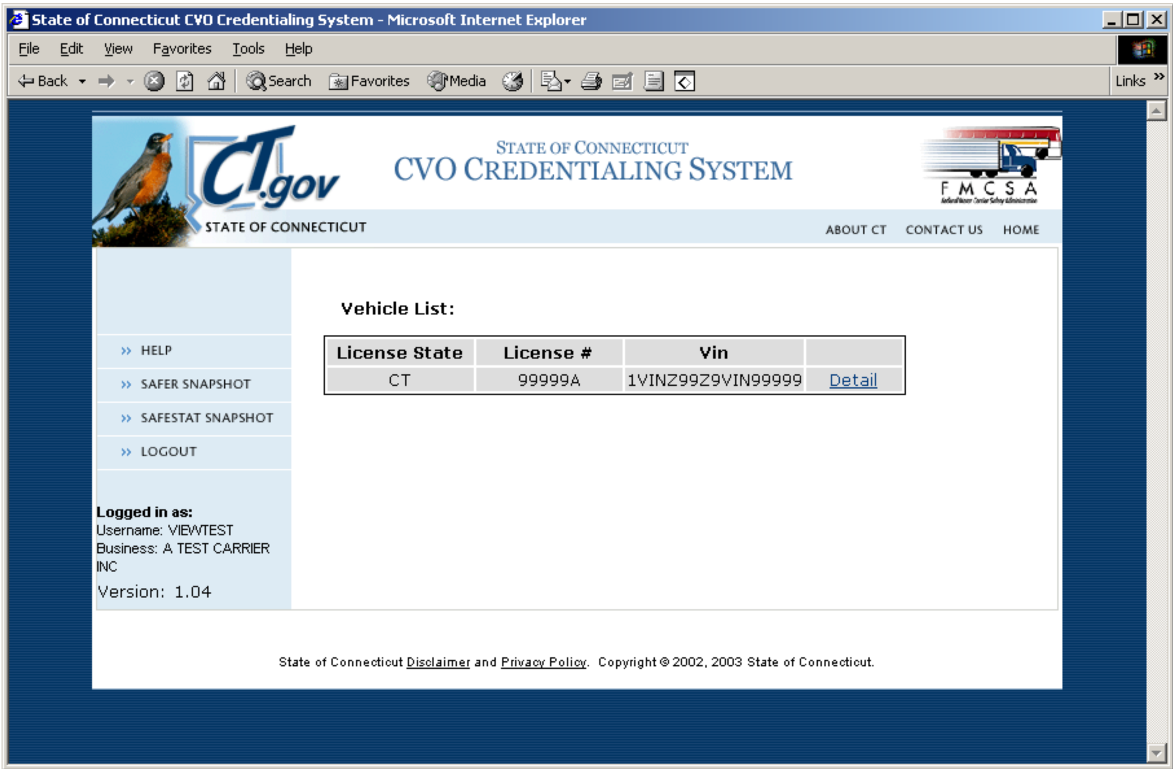

At the bottom of the carrier information screen is a link to view the carrier's vehicle list as shown in Figure 7.4.

# Figure 7.4 Vehicle Link on Carrier Information Screen




Clicking "View Carrier's Vehicle List" will display the vehicles associated with the carrier's fleet as shown in Figure 7.5. All of a carrier's Connecticut-based IRP-registered vehicles should appear on this list. Additional vehicles will be associated with the carrier based on the data provided by FMCSA and other jurisdictions.

## Figure 7.5 Vehicles for a Carrier

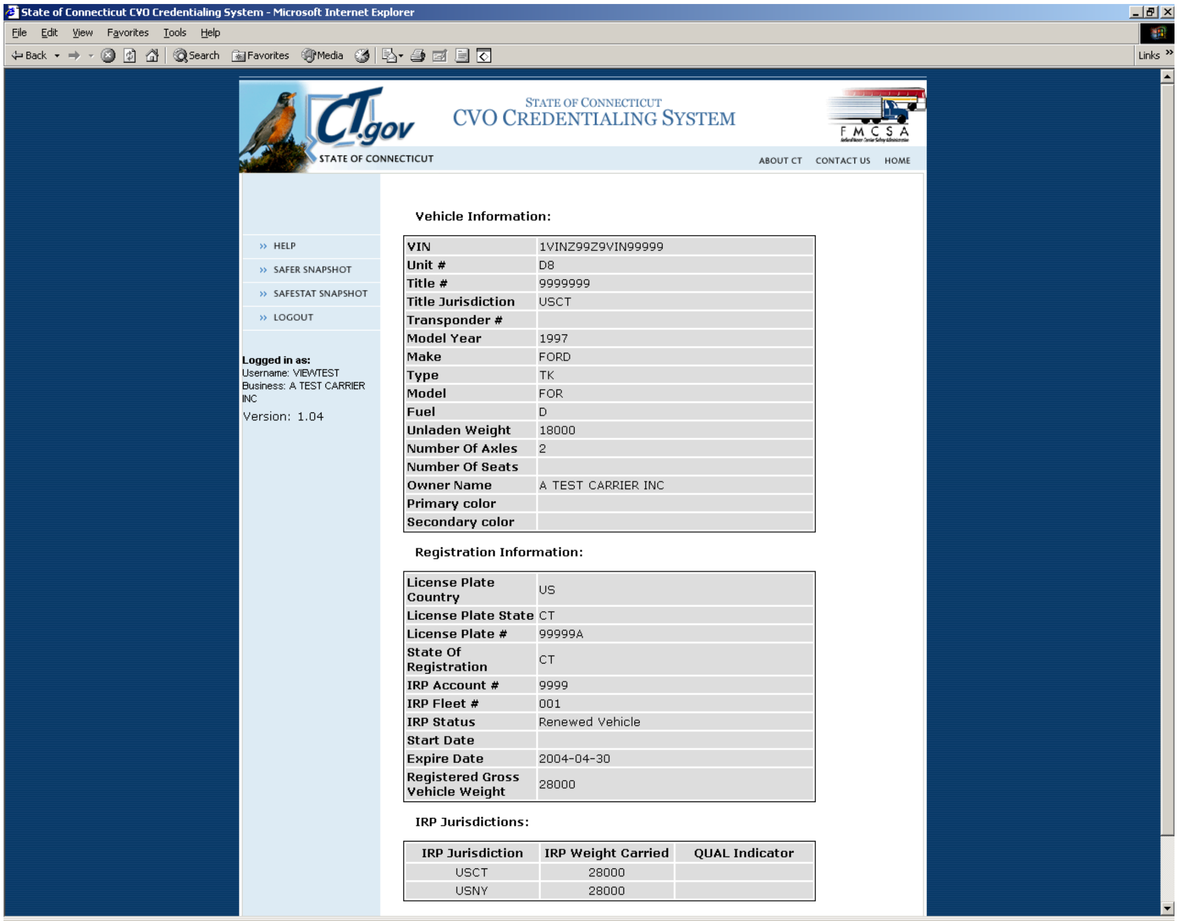



Clicking the "Detail" link on the vehicle list page will display detailed information for the vehicle as shown in Figure 7.6.

The detailed vehicle information includes:

- **Vehicle Information –** VIN, unit number, title information, transponder, year, make, model, type, registered weight, number of axles, number of seats, owner's name, primary color, and secondary color;
- **Registration Information –** License plate country, license plate state, license plate number, registration state, IRP account number, IRP fleet number, IRP status, IRP start date, IRP expire date, and registered gross vehicle weight;
- **IRP Jurisdictions –** IRP-registered jurisdictions, IRP weight carried by jurisdiction, and "QUAL Indicator"; and
- **OS/OW permits** associated with the carrier also will be contained in the snapshot scheduled for April 2004.

## Figure 7.6 Detailed Vehicle Information




The user also can display his/her company's information stored in the FMCSA Safety and Fitness Electronic Records (SAFER) and Safety Status (SAFESTAT) systems. To access the SAFER system, click "View SAFER Snapshot" in the user options menu. To access the SAFESTAT system, click "View SAFESTAT Snapshot" in the user options menu. Each of these systems will be displayed in a separate window. To exit the SAFER or SAFESTAT snapshots, close the browser window in which they were displayed.

# 8.0 Administration

The CVO Credentialing System is deployed on shared WebSphere 4 servers in Connecticut. There are two environments maintained on two separate servers.

1. The testing/training environment exists on a shared staging server. The uniform resource locator (URL) of the CVO Credentialing System on the shared staging server is https://vvv.cvisn.state.ct.us/ct.

2. The production environment exists on a shared production server. The URL on the production server is https://www.cvisn.state.ct.us/ct.

## 8.1 Installation

CS is responsible for all development activities associated with the CVO Credentialing System. Development occurs at the CS' offices. Prior to installing the application in Connecticut, CS produces the deployment files, deploys the application on a development server, and performs regression testing.

When CS is ready to deploy the application on the Connecticut staging server, the following deployment process is used:

- CS connects to the State VPN.

- CS opens an FTP connection to the shared WebSphere staging server at 159.247.3.167.

- CS uploads the ct-portal-ear.ear and ct-ifta-ear.ear files. EAR stands for Enterprise Archive, which contains a Java Enterprise application for WebSphere. Both the CVO Credentialing System, also called $\text{PORTAL}_{\text{CS}}$, and the $\text{IFTA}_{\text{CS}}$ Credential Web Application, described in the *IFTA User Interface Manual*, are deployed simultaneously. These files are placed in E:\inetpub\cvisn.

- CS contacts the Connecticut Department of Information Technology (DOIT) at app.hosting@po.state.ct.us and requests that the applications be deployed using the script install_cvisn_apps.bat, which may be found in E:\WebSphere\AppServer\scripts.

- DOIT performs the deployment and informs CS when the deployment is complete.

- CS checks the deployment and performs installation testing.

When CS is ready to deploy the application on the Connecticut production server, CS contacts DOIT at app.hosting@po.state.ct.us and requests that the staging application be migrated to the production server. DOIT performs this migration at the next change control cycle and informs CS when the migration is complete. CS checks the deployment and performs installation testing.

## 8.2 Configuration

The CVO Credentialing System requires access to shared resources, including the three CVISN/PRISM databases and the State's SMTP server. Information regarding these resources is maintained within the WebSphere environment. There are five items that must be established as part of the CVO Credentialing System configuration:

- Connection to the $\text{PORTAL}_{\text{CS}}$ database;
- Connection to the IFTA database;
- Connection to the $\text{CVIEW}_{\text{CS}}$ database;
- Connection to the State's SMTP server; and
- JVM system property used to distinguish between release, i.e., staging, and production environments.

Each configuration item is described below.

For the $\text{PORTAL}_{\text{CS}}$ database connection, create a new entry under Resources: JDBC Drivers: *driver:* Data Sources from within the WebSphere Administrator's Console. The actual name of the JDBC driver shown in italics is specific to the WebSphere environment. For the CVO Credentialing System this value usually will be Oracle JDBC Driver. Set the parameters of the data source as shown in Table 8.1.

### Table 8.1 $\text{PORTAL}_{\text{CS}}$ Data Source Parameters

| Parameter | Value |
|---|---|
| Name | portalDataSource |
| JNDI Name | jdbc/portalDataSource |
| Description | Oracle Data Source for $\text{PORTAL}_{\text{CS}}$ Database |
| Database Name | portal |
| Default User ID | portal |
| Default Password | portalpwd |

## Table 8.1 PORTAL$_{CS}$ Data Source Parameters (continued)

| Parameter | Value |
|---|---|
| Minimum Pool Size | 0 |
| Maximum Pool Size | 10 |
| Connection Timeout | 30 |
| Idle Timeout | 295 |
| Orphan Timeout | 295 |
| Statement Cache Size | 100 |
| Disable Auto Connection Cleanup | Unchecked |

Under Properties… -> Driver-Specific Settings, create a new entry with Name = URL, Type = String and Value = jdbc:oracle:thin:@159.247.104.xx:1521:portal. For "xx," use 35 for the staging server and 34 for the production server.

For the IFTA database connection, create a new entry under Resources: JDBC Drivers: *driver*: Data Sources from within the WebSphere Administrator's Console. Set the parameters of the data source as shown in Table 8.2.

## Table 8.2 IFTA Data Source Parameters

| Parameter | Value |
|---|---|
| Name | iftaDataSource |
| JNDI Name | Jdbc/iftaDataSource |
| Description | Oracle Data Source for IFTA Database |
| Database Name | ifta |
| Default User ID | ifta |
| Default Password | iftapwd |
| Minimum Pool Size | 0 |
| Maximum Pool Size | 10 |
| Connection Timeout | 30 |
| Idle Timeout | 295 |
| Orphan Timeout | 295 |
| Statement Cache Size | 100 |
| Disable Auto Connection Cleanup | Unchecked |

Under Properties… -> Driver-Specific Settings, create a new entry with Name = URL, Type = String and Value = jdbc:oracle:thin:@159.247.104.xx:1521:ifta. For “xx,” use 35 for the staging server and 34 for the production server.

For the CVIEW$_{CS}$ database connection, create a new entry under Resources: JDBC Drivers: *driver:* Data Sources from within the WebSphere Administrator’s Console. Set the parameters of the data source as shown in Table 8.3.

### Table 8.3 CVIEW$_{CS}$ Data Source Parameters

| Parameter | Value |
|---|---|
| Name | cviewDataSource |
| JNDI Name | jdbc/cviewDataSource |
| Description | Oracle Data Source for CVIEW$_{CS}$ Database |
| Database Name | cview |
| Default User ID | cview |
| Default Password | Cviewpwd |
| Minimum Pool Size | 0 |
| Maximum Pool Size | 10 |
| Connection Timeout | 30 |
| Idle Timeout | 295 |
| Orphan Timeout | 295 |
| Statement Cache Size | 100 |
| Disable Auto Connection Cleanup | Unchecked |

Under Properties… -> Driver-Specific Settings, create a new entry with Name = URL, Type = String and Value = jdbc:oracle:thin:@159.247.104.xx:1521:cview. For “xx,” use 35 for the staging server and 34 for the production server.

For the SMTP server connection, create a new entry under Resources: Mail Providers: Default Mail Provider: Mail Sessions from within the WebSphere Administrator’s Console. Set the parameters of the mail session as shown in Table 8.4.

## Table 8.4 SMTP Parameters

| Parameter | Value |
|---|---|
| Name | mail/portalMailSession |
| JNDI Name | mail/portalMailSession |
| Description | Connection to State SMTP Server |
| Mail From | 93992@po.state.ct.us |
| Mail Transport Host | po.state.ct.us |
| Mail Transport Protocol | smtp |

The CVO Credentialing System must have a way to determine if it is running within the staging or production environment. This is accomplished through a system property. Create a new entry under Properties: JVM Settings: System Properties from within the WebSphere Administrator's Console. Set the parameters of the system property as shown in Table 8.5.

## Table 8.5 JVM System Property

| Parameter | Value |
|---|---|
| Name | deployment.CTCVISN |
| Value | release (for staging server) or production (for production server) |

All parameter values are case-sensitive.

## 8.3 Troubleshooting

The CVO Credentialing System produces two log files. These files are:

- CVISN_APP_stdout.txt – Contains messages generated by the CVO Credentialing System and the IFTA$_{CS}$ Credential Web Application.
- CVISN_APP_stderr.txt – Contains messages generated by the WebSphere environment.

These files are created on the shared Connecticut WebSphere servers in the directory E:\WebSphere\AppServer\logs. New information is appended to the end of these files. Old information should be purged once every six to 12 months, depending on the number of users and transactions processed.

These logs should be reviewed on a periodic basis and in response to specific problems reported by users. CS presently has access to the files on the shared WebSphere staging server. CS will request these files from DOIT for the shared WebSphere production server.

# Appendix A

*Portal*$_{CS}$

# PORTAL$_{CS}$

This section describes the physical design of PORTAL$_{CS}$, the web-based Portal for online access to commercial vehicle operations in Connecticut. PORTAL$_{CS}$ will include the following pages:

- **PORTAL$_{CS}$ Login Page –** This is the first page displayed when a user arrives at PORTAL$_{CS}$. This is where a user who has an existing account may log into the credentialing system by entering his/her username and password.
- **Register as a Carrier Page –** This page allows a carrier user to establish an account with the State.
- **Register as a Service Bureau Page –** This page allows the service bureau user to establish an account with the State.
- **Forgot Your Password? Page –** This page allows a user who has forgotten his/her password to reset it.
- **Help Page (prior to logging in) –** This page is available on the Login, Register, and Forgot Your Password? Pages. It displays in a separate browser window instructions for logging in, self-registration, and resetting one's password.
- **PORTAL$_{CS}$ Main Menu Page –** This page is displayed following a successful login. It displays a number of options that a user may select in order to view data, transfer to a credential web application, update registration information, and manage subaccounts.
- **Help Page (within PORTAL$_{CS}$) –** This page is available from all locations within the credentialing system. It displays in a separate browser window consolidated help for using the credentialing system.
- **Edit My Account Page –** This page allows a user who has logged in to change current registration information.
- **Manage User Accounts and Subaccount Management Pages –** These pages allow a user who has logged in to create a new subaccount, disable or enable a subaccount, or change subaccount information.
- **View Carrier and Vehicle Information Pages –** These pages allow carrier users who have logged in to confirm information stored in CVIEW$_{CS}$, and State users to support regulatory and enforcement activities. Carrier, vehicle, and permit information are included on the various pages.

Authorized users may transfer to the $IFTA_{CS}$ credential web application, MVS/Express web application (IRP credentials), and e-PASS web application (oversize/overweight permits) from the $PORTAL_{CS}$ Main Menu.

Pages of the $IFTA_{CS}$ credential web application are fully described in Section 11.3 of the CI/CVIEW Detailed (Physical) Design. Page details for the MVS/Express and e-PASS web applications will be provided by the Award 2 and Award 3 vendors, respectively.

## A.1 Overview

$PORTAL_{CS}$ serves as the Credentialing Interface Portal for all credentials selected by the Connecticut CVISN agencies. $PORTAL_{CS}$ will provide the following functionality:

- Single source of user authentication;
- Account and security management;
- Dynamic menu based on user privileges;
- Link to carrier and vehicle snapshots;
- Link to IRP credential web application;
- Link to $IFTA_{CS}$ credential web application;
- Link to OS/OW permit web application; and
- Centralized interface for electronic payments.

Figure A.1 illustrates the $PORTAL_{CS}$ structure and functionality.

Note: The link the OS/OW permit web application and processing of ACH payments will be implemented as part of interim Release 1, scheduled for April 2004.

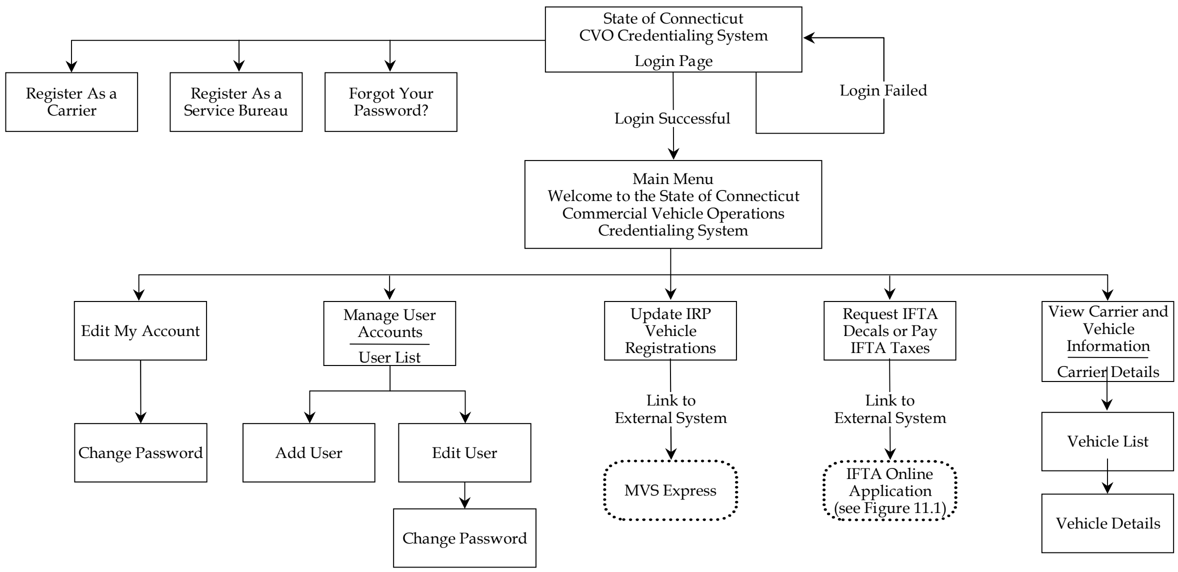
## A.2 Process Flow

### A.2.1 $PORTAL_{CS}$ Login

A user arriving at the $PORTAL_{CS}$ Login Page is presented the following operations:

- Login using an existing account;
- Self-register as a carrier;
- Self-register as a service bureau; and
- Request that a forgotten password be reset.

## Figure A.1 Portal$_{CS}$ Structure

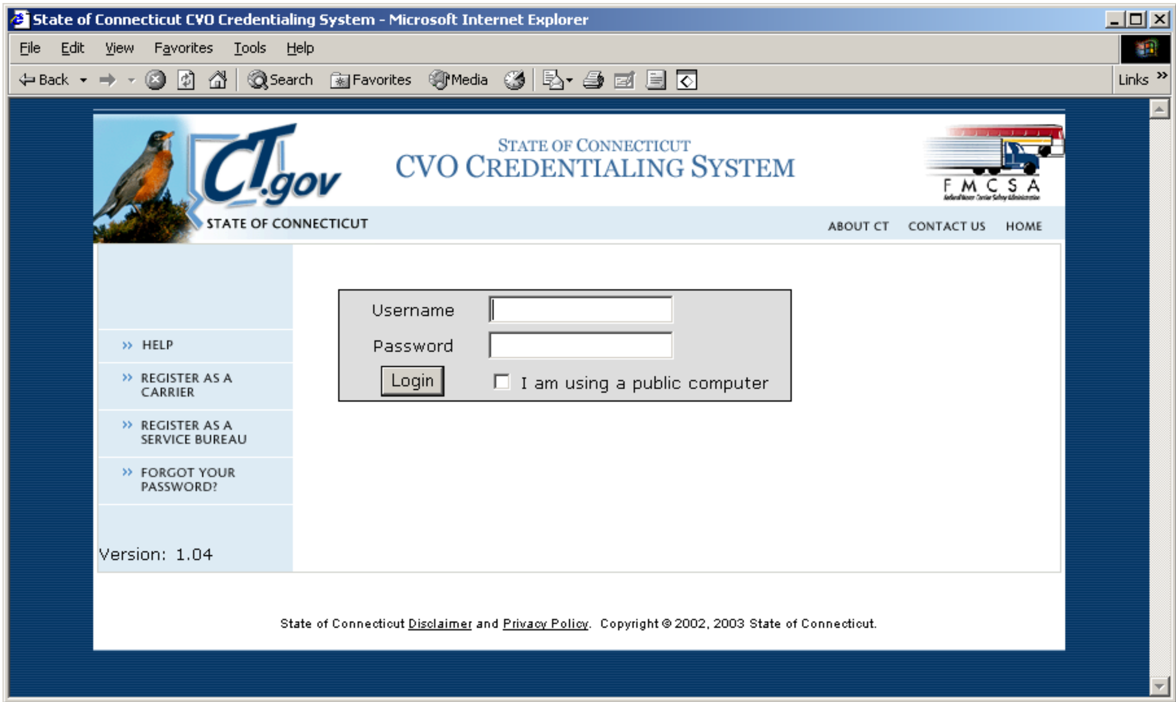



Notes

1. Once logged into PORTALcs, a user may access the main menu by clicking "home" from any page
2. A user may access SAFER and SafeStat from any "View Carrier and Vehicle Information" page
3. A user can logout of PORTALcs from any screen
4. "Help" is available to users on every screen

A Help hyperlink also is available with help on these operations. Figure A.2 illustrates the PORTAL$_{CS}$ Login Page.

## Figure A.2 PORTAL$_{CS}$ Login Page




### *Login Using an Existing Account*

A user with an existing account may log into the CVO Credentialing System by entering his/her username and password.

The Login Page includes:

- Login button, which will run a match of the username and password with entries in the PORTAL$_{CS}$ database of users. Following a successful match, a user will be directed to the PORTAL$_{CS}$ Main Menu. Username and login time/date will be recorded in the USER_LOGIN table (see Section A.4.6).

- Help hyperlink, which will display in a separate browser window instructions for login, self-registration, and resetting one's password.

- Register as a Carrier hyperlink, which will transfer control to the page that allows a carrier user to establish an account with the State.

- Register as a Service Bureau hyperlink, which will transfer control to the page that allows the service bureau user to establish an account with the State.

- Forgot Your Password? hyperlink, which will transfer control to the page that allows the user who has forgotten his/her password to reset it.

- Home hyperlink, which will keep the user on the Login Page.

A user also may select the checkbox indicating his/her use of a public computer from the Log-in screen. If this setting is selected, a user is logged into the Portal at a higher security level, resulting in a 10-minute session timeout – rather than the standard four hours.

### *Self-Register as a Carrier*

When the user clicks on the Register as a Carrier hyperlink from the $\text{PORTAL}_{\text{CS}}$ Login Page, control is transferred to the Register as a Carrier Page. This page allows the user to enter all the information required to establish a Portal account. This master account is a carrier's main account. Figure A.3 illustrates the Self-Register as a Carrier Page.

The page includes:

- Register button, which will submit the registration form. If no errors are encountered, the registration is accepted and the user is returned to the Login Page. The act of registering does not log in the user. If errors are encountered with the registration (e.g., required fields are not filled in) the user is presented with a list of errors along with the form that was originally displayed. A user must correct the errors before the registration is accepted. The operation to Register as a Carrier writes a profile to the Portal database.

- Reset button, which will clear all fields of entered information. This allows the user to start anew with the registration.

- Cancel button, which will cancel the operation and transfer control to the Login Page.

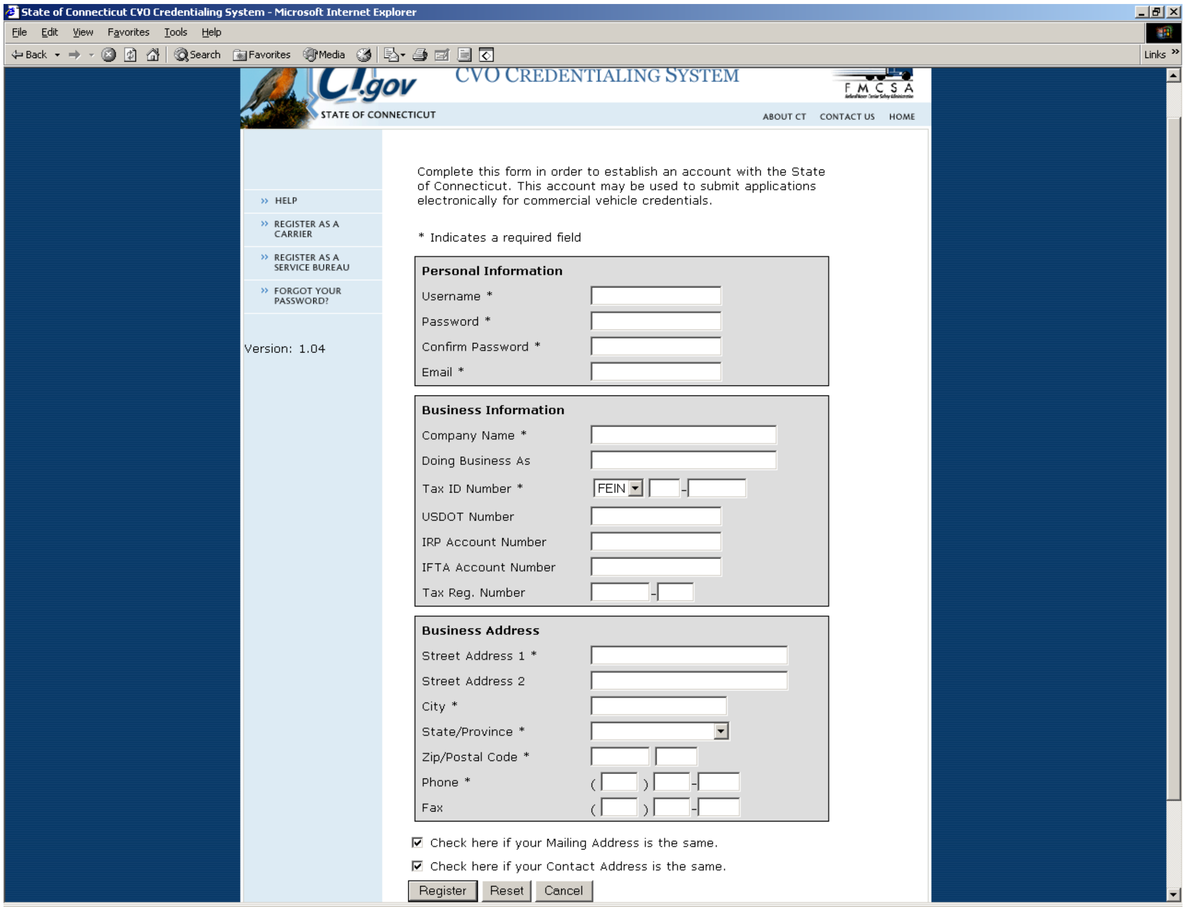
- Help hyperlink, which will display in a separate browser window instructions for login, self-registration, and resetting one's password.

- Register as a Service Bureau hyperlink, which will transfer control to the page that allows the service bureau user to establish an account with the Portal.

- Forgot Your Password? hyperlink, which will transfer control to the page that allows the user who has forgotten his/her password to reset it.

- Home hyperlink, which will transfer control to the Login Page.

## Figure A.3 Self-Register as a Carrier Page

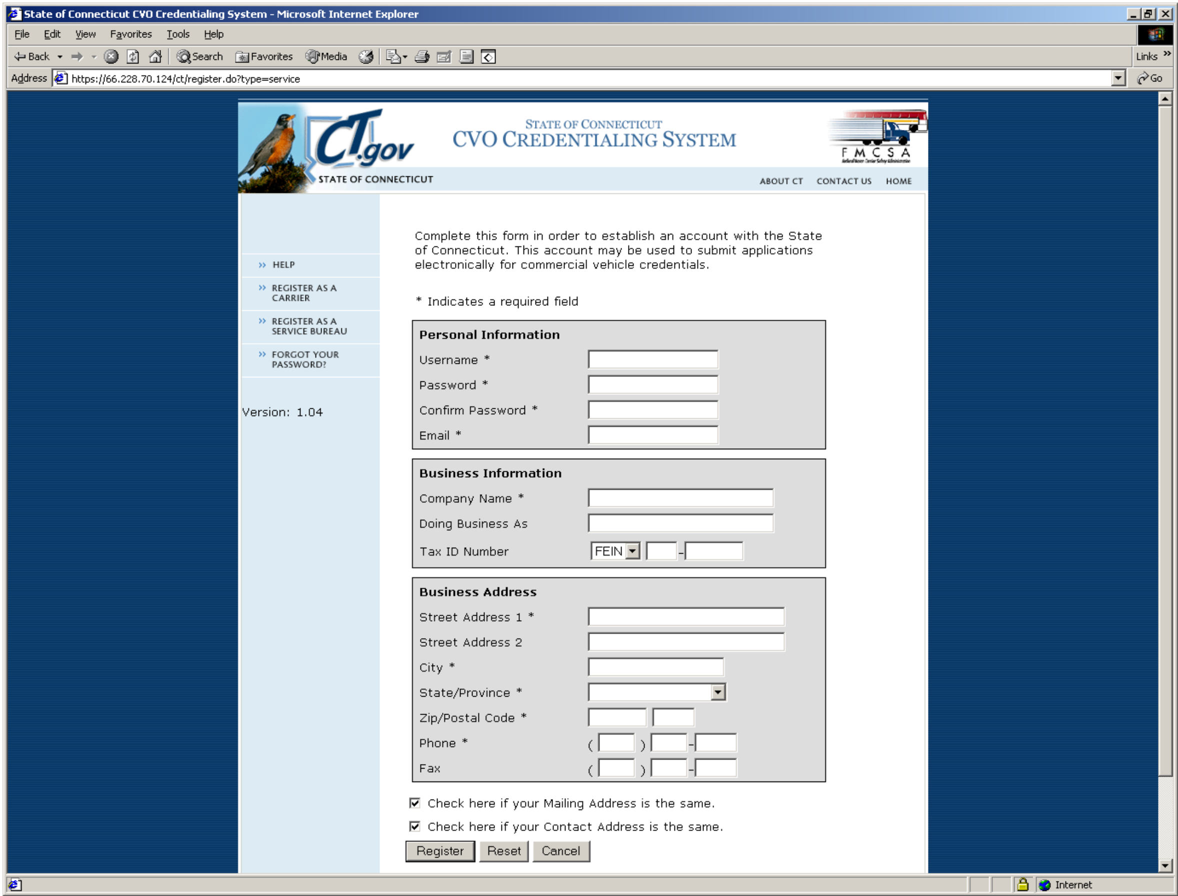



Once a user has successfully registered, he/she may log into the Portal by providing his/her username and password on the Portal login screen. If this username and password match entries in the PORTAL$_{CS}$ database of users, the user will be directed to the Portal Main Menu. If this username and password does not match entries in the PORTAL$_{CS}$ database of user, an error message will be displayed and the user will be returned to the Login Page.

### *Self-Register as a Service Bureau*

When the user clicks on the Register as a Service Bureau hyperlink from the PORTAL$_{CS}$ Login Page, control is transferred to the Register as a Service Bureau Page. This page allows the user to enter all the information required to establish a Portal account. This master account is a service bureau's main account. Figure A.4 illustrates the Self-Register as a Service Bureau Page.

## Figure A.4 Self-Register as a Service Bureau Page




The page includes:

- Register button, which will submit the registration form. If no errors are encountered, the registration is accepted and the user is returned to the Login Page. The act of registering does not log in the user. If errors are encountered with the registration (e.g., required fields are not filled in) a user is presented with a list of errors along with the form that was originally displayed. A user must correct the errors before the registration is accepted. The operation to Register as a Service Bureau writes a profile to the Portal database.

- Reset button, which will clear all fields of entered information. This allows a user to start anew with the registration.

- Cancel button, which will cancel the operation and transfer control to the Login Page.

- Help hyperlink, which will display in a separate browser window instructions for login, self-registration, and resetting one's password.

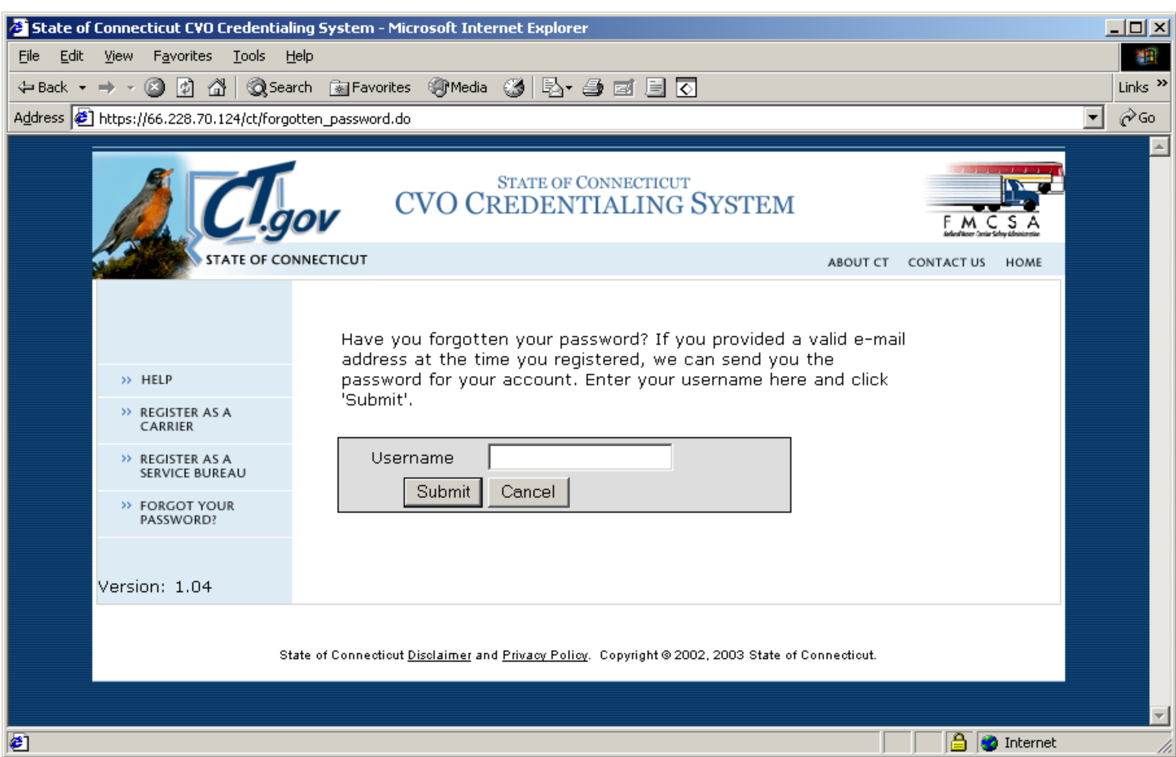
- Register as a Carrier hyperlink, which will transfer control to the page that allows a carrier user to establish an account with the State.
- Forgot Your Password? hyperlink, which will transfer control to the page that allows a user who has forgotten his/her password to reset it.
- Home hyperlink, which will transfer control to the Login Page.

Once a user has successfully registered, he/she may log into the Portal by providing his/her username and password on the Portal login screen. If this username and password match entries in the PORTAL$_{CS}$ database of users, a user will be directed to the Portal Main Menu. If this username and password does not match entries in the PORTAL$_{CS}$ database of user, an error message will be displayed and the user will be returned to the Login Page.

### Request a Forgotten Password

When a user clicks on the Forgot Your Password? hyperlink from the PORTAL$_{CS}$ Login Page, control is transferred to the Forgot Your Password? Page. This page allows a user who has forgotten his/her password to reset it. A user is prompted to enter his/her username in order to receive his/her password at the e-mail address associated with the username and stored in a user's profile. Figure A.5 illustrates the Request a Forgotten Password Page.

## Figure A.5 Request a Forgotten Password Page



The page includes:

- Submit button, which will process the operation to reset the password for the account and send it to the e-mail address that is associated with the username and stored in the Portal. A user is returned to the Login Page.
- Cancel button, which will cancel the operation and transfer control to the Login Page.
- Help hyperlink, which will display instructions for login, self-registration, and resetting one's password in a separate browser window.
- Register as a Carrier hyperlink, which will transfer control to the page that allows the carrier user to establish an account with the State.
- Register as a Service Bureau hyperlink, which will transfer control to the page that allows the service bureau user to establish an account with the State.
- Home hyperlink, which will transfer control to the Login Page.

### *Help*

When a user clicks on the Help hyperlink from the PORTAL$_{CS}$ Login Page, a separate browser window is opened that displays instructions for submitting information on the Login, Register as a Carrier, Register as a Service Bureau, and Forgot Your Password? Pages.

## A.2.2 PORTAL$_{CS}$ Main Menu Access

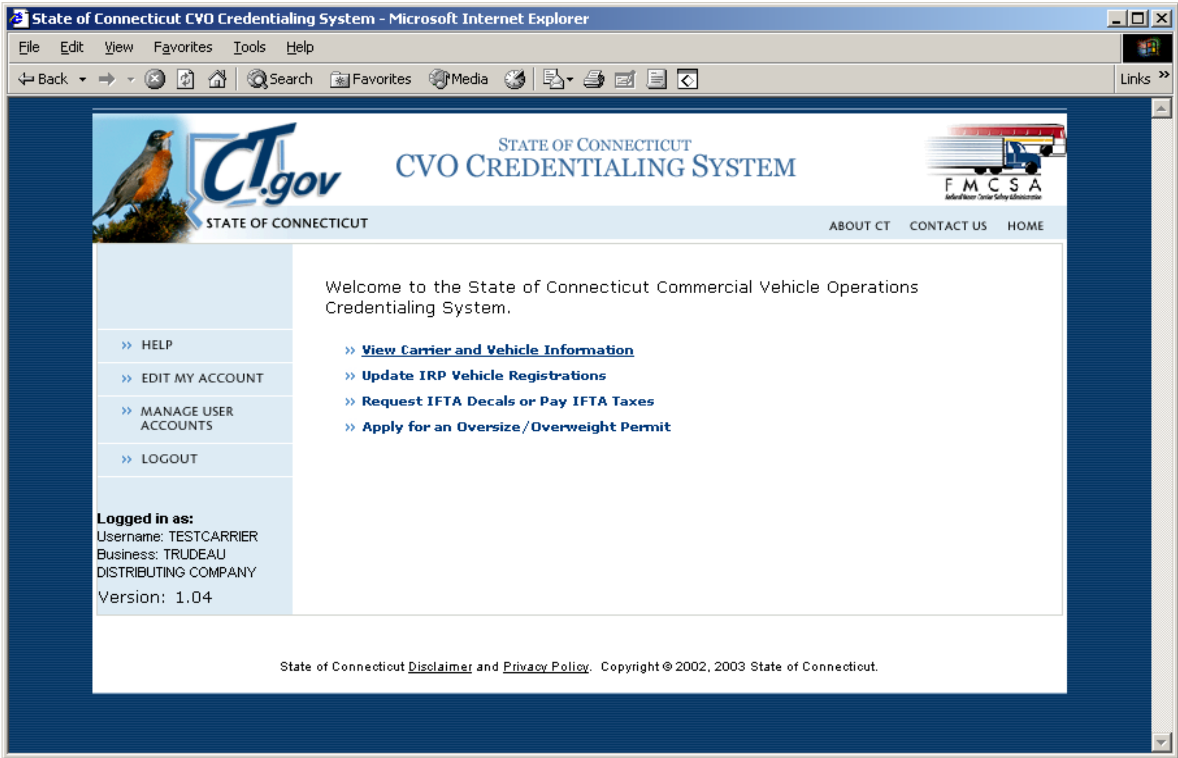
### *Main Menu*

If a user's username and password match entries in the PORTAL$_{CS}$ database of users, he/she will be directed to the Portal Main Menu. Figure A.6 illustrates the PORTAL$_{CS}$ Main Menu Page.

The first page that is displayed greets a user and includes a dynamic list of allowable activities based on security flags stored in the user Portal profile. These security flags have default values according to agency business processes and whether a user is a carrier or a service bureau. (See Section A.10) Upon receiving a request from the State, Cambridge Systematics will update a user's security flags.

Up to four options are presented to a user on the menu page – depending on a user's privileges. Each of these options transfers a user to another web application or another position in the Portal where additional data can be viewed or additional functions performed.

## Figure A.6 PORTAL$_{CS}$ Main Menu Page




The four options include:

- View Carrier and Vehicle Information hyperlink that allows an authorized carrier or State user to view snapshot information;

- Update IRP Vehicle Registrations hyperlink that transfers an authorized carrier or service bureau user to the MVS/Express web application;

- Request IFTA Decals or Pay IFTA Taxes hyperlink that transfers an authorized carrier or service bureau user to the IFTA$_{CS}$ credential web application, including to the RPC; and

- Apply for an Oversize/Overweight Permit hyperlink that transfers an authorized carrier or service bureau user to the e-PASS web application.

As noted above, the link to the OS/OW permit hyperlink will be implemented as part of interim Release 1.

The menu page also includes the following hyperlinks located in the side bar:

- Help hyperlink that provides help about the credentialing system;
- Edit My Account hyperlink that allows a user to edit the information provided during PORTAL$_{CS}$ registration;
- Manage User Accounts hyperlink that allows a master account to manage its subaccounts; and
- Logout hyperlink that closes the session and returns a user to the Login Page.

**In the upper right bar of every page within the credentialing system is a Home hyperlink that returns a user to the Portal Main Menu.**

### *View Carrier and Vehicle Information*

The View Carrier and Vehicle Information hyperlink appears only if the View Carrier Information flag is set to Y for the current user in the PORTAL$_{CS}$ database of users. The View Carrier Information flag is set to N by default when a new master account is created. The State can direct that this permission be enabled for carriers or State users on a case-by-case basis after the master account has been created.

Carriers will use this option to confirm information stored in CVIEW$_{CS}$. State law enforcement personnel will use this option to support inspection and enforcement activities. Figure A.7 illustrates the Carrier Information Page accessible through PORTAL$_{CS}$.

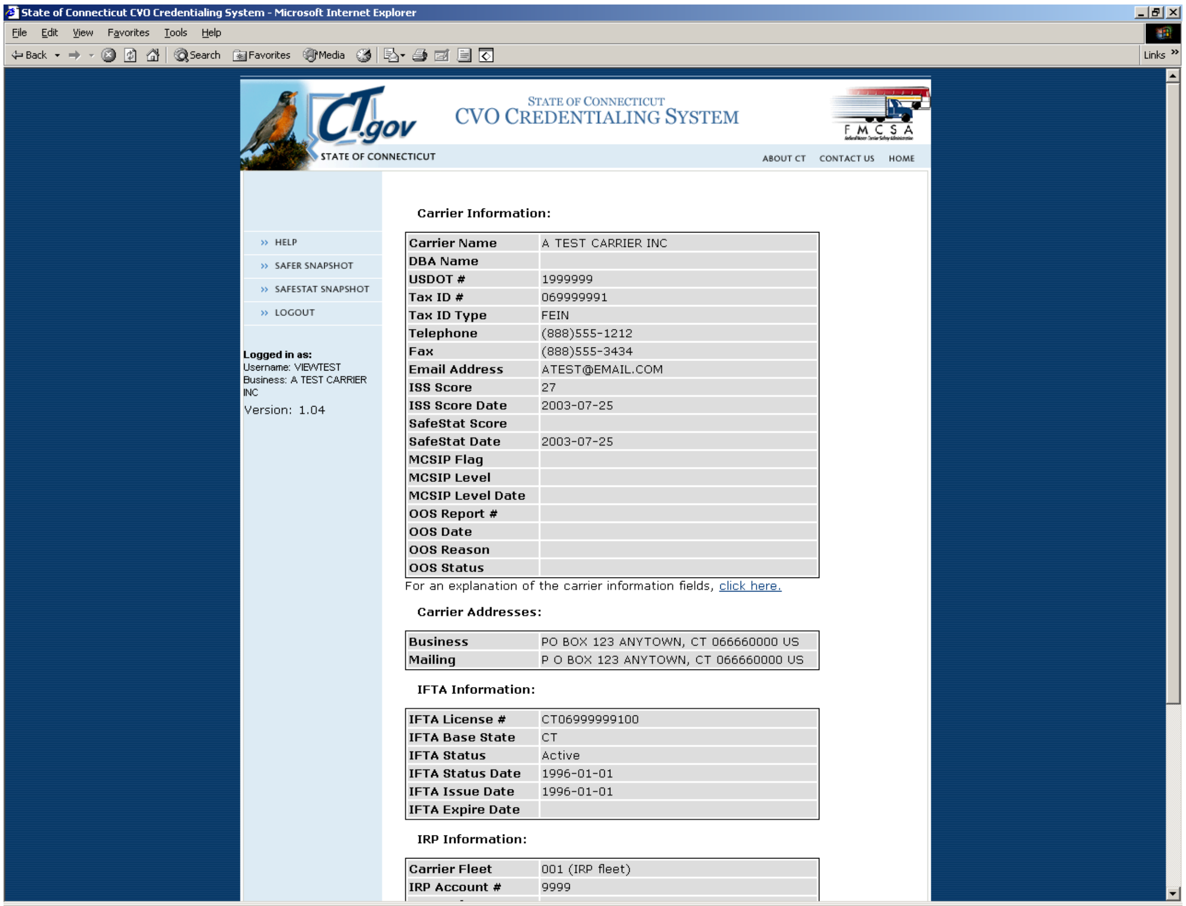
This option will not be available to service bureau accounts. Service bureaus will not be authorized to view information about any carriers, including those that they represent. If a carrier desires to have a service bureau view its snapshot information, the carrier must create a separate subaccount with its master account, grant permission to this subaccount to "View Carrier" (information), and provide this subaccount information to the service bureau.

The carrier also must change or disable the subaccount when they no longer wish to allow the service bureau access to its snapshot. Each carrier that wishes to allow a service bureau to view its snapshot information must perform this operation and the service must use the appropriate subaccount information in order to view a carrier's snapshot. (Manage User Accounts section below provides information on creating, disabling, and editing subaccounts.)

Clicking on the View Carrier and Vehicle Information hyperlink will display the Carrier Snapshot Details. Upon clicking this link, a user is presented with a series of information about the carrier. This page shows information from the Connecticut CVIEW$_{CS}$ carrier snapshot for the current user. For a carrier user, this page can be displayed immediately because the information necessary to retrieve the snapshot is associated with a user in the PORTAL$_{CS}$ database of users. The FEIN or SSN provided by the carrier when the master account is created is the key used to retrieve the snapshot from the CVIEW$_{CS}$ database.

When an authorized State user accesses this function, an intermediate page will appear requesting carrier identifying information, e.g., U.S. DOT number, FEIN or SSN. This information must be supplied each time a snapshot is retrieved.

## Figure A.7 Carrier Information Page




Authorized State personnel may view the snapshot for any carrier in the CVIEW$_{CS}$ database. If the carrier identifying information provided by a user equates to one and only one carrier in the CVIEW$_{CS}$ database, the Carrier Snapshot Detail Page for that carrier will be displayed. Otherwise an error message will be displayed and the user can enter new identifying information. There is no case in which one of these numbers can result in the retrieval of multiple snapshots because the identifiers are unique to a carrier in CVIEW$_{CS}$.

If the Carrier Snapshot Detail information cannot be located in the CVIEW$_{CS}$ database (by FEIN/SSN for a carrier or U.S. DOT/FEIN/SSN for a State user), PORTAL$_{CS}$ will display the message, "Sorry, no carrier and vehicle information found for this carrier!" A user then will be directed back to the Portal Main Menu. State users will be allowed to enter different retrieval parameters. OS/OW permit information will be added to the Carrier Snapshot Detail Page, if appropriate, as part of the interim Release 1.

The Carrier Snapshot Detail Page includes:

- View Carrier's Vehicle List hyperlink, which will transfer control to the Vehicle List Page.
- Help hyperlink, which will open a separate browser window displaying a consolidated Help Page for the credentialing system.
- SAFER Snapshot hyperlink, which will transfer a user to the SAFER web site for information on the current carrier.
- SafeStat Snapshot hyperlink, which will transfer a user to the SafeStat web site for information on the current carrier.
- Logout hyperlink, which will transfer control to the $\text{PORTAL}_{\text{CS}}$ Login Page.
- Home hyperlink, which will transfer control to the $\text{PORTAL}_{\text{CS}}$ Main Menu.

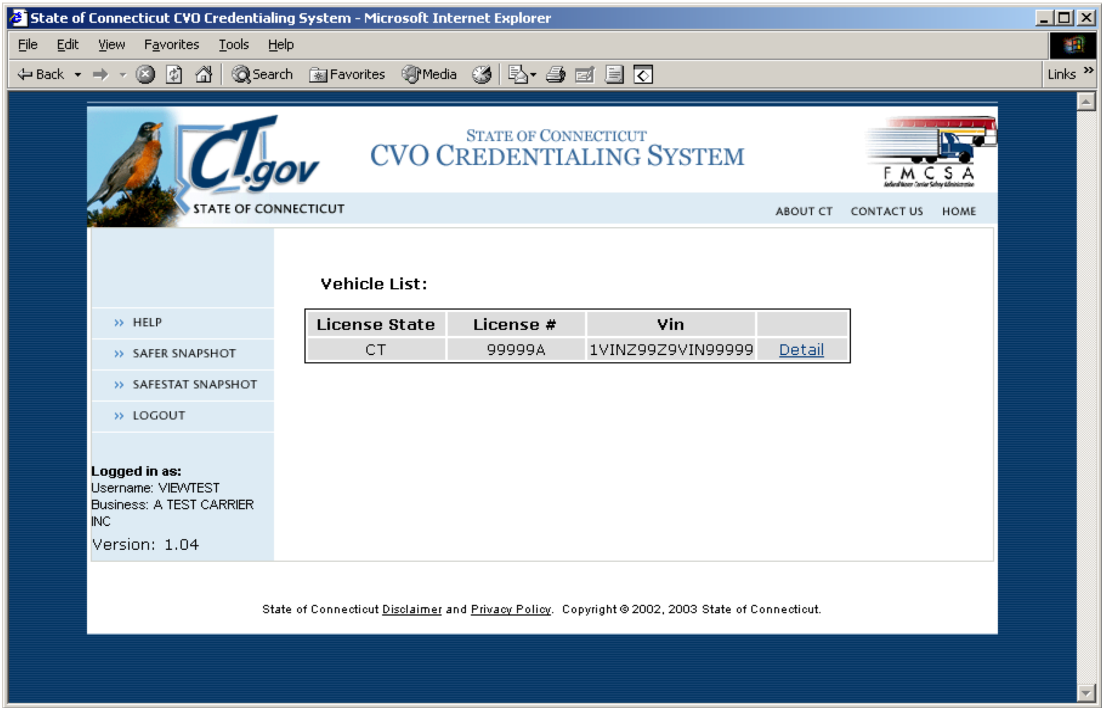
The Vehicle List Page displays the list of vehicles for the carrier. Only vehicles for which a relationship with the carrier has been identified (i.e., through information supplied by the IRP system, transponder registration system, or PRISM Target File) will be reported. If no vehicles are found for the carrier, $\text{PORTAL}_{\text{CS}}$ will display the message, "Sorry, no vehicles found for this carrier!" Figure A.8 illustrates the Vehicle List Page.

The page includes:

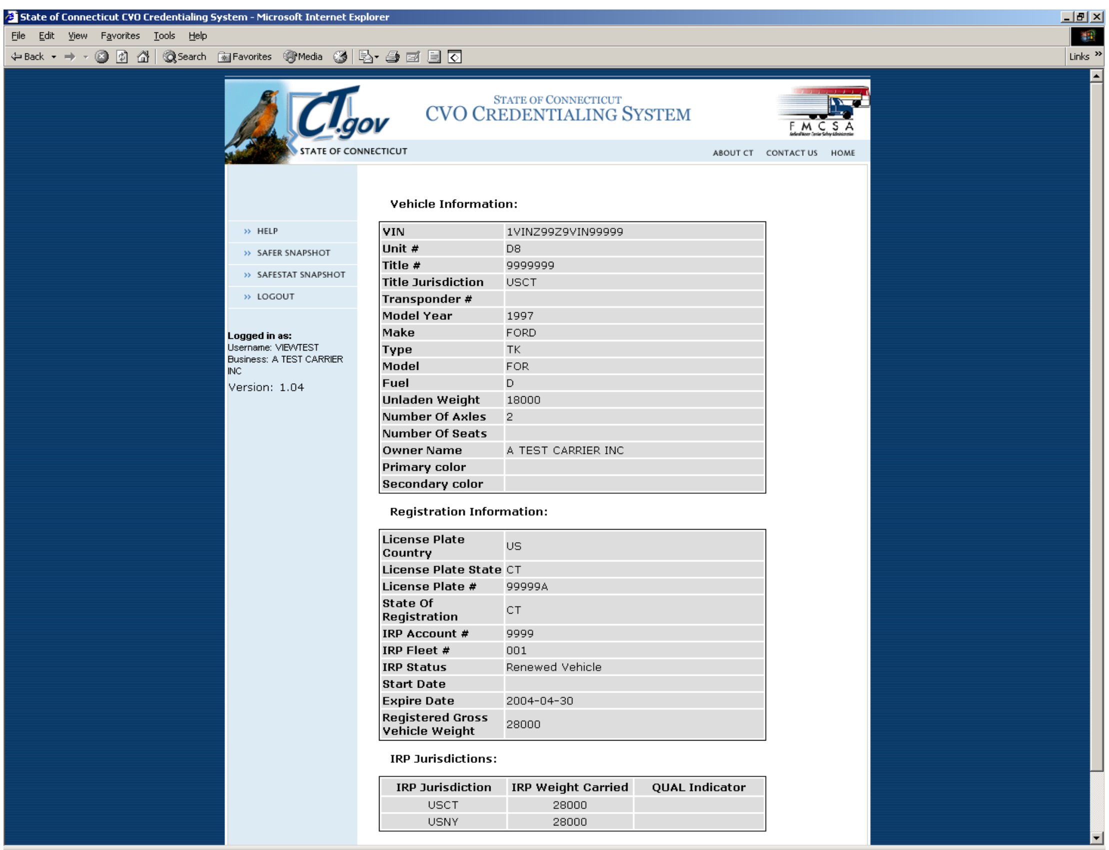
- Detail hyperlink for each vehicle, which will transfer control to the Vehicle Snapshot Detail Page for the vehicle.
- Help hyperlink, which will open a separate browser window displaying a consolidated Help Page for the credentialing system.
- SAFER Snapshot hyperlink, which will transfer a user to the SAFER web site for information on the current carrier.
- SafeStat Snapshot hyperlink, which will transfer a user to the SafeStat web site for information on the current carrier.
- Logout hyperlink, which will transfer control to the $\text{PORTAL}_{\text{CS}}$ Login Page.
- Home hyperlink, which will transfer control to the $\text{PORTAL}_{\text{CS}}$ Main Menu.

The Vehicle Snapshot Detail Page displays the data for one vehicle drawn from the Connecticut $\text{CVIEW}_{\text{CS}}$ database. This allows a user to view a detailed snapshot for that vehicle. There is no circumstance in which a selected vehicle snapshot will not be found once a vehicle is selected on the Vehicle List Page. Figure A.9 illustrates the Vehicle Snapshot Detail Page.

# Figure A.8 Vehicle List Page




# Figure A.9 Vehicle Snapshot Detail Page



The page includes:

- Help hyperlink, which will open a separate browser window displaying a consolidated Help Page for the credentialing system.
- SAFER Snapshot hyperlink, which will transfer a user to the SAFER web site for information on the current carrier.
- SafeStat Snapshot hyperlink, which will transfer a user to the SafeStat web site for information on the current carrier.
- Logout hyperlink, which will transfer control to the $\mathrm{PORTAL_{CS}}$ Login Page.
- Home hyperlink, which will transfer control to the $\mathrm{PORTAL_{CS}}$ Main Menu.

### *Update IRP Vehicle Registrations*

The Update IRP Vehicle Registrations hyperlink appears only if the Access IRP flag is set to Y for the current user in the $\mathrm{PORTAL_{CS}}$ database of users and a non-blank MVS/Express username has been added to the $\mathrm{PORTAL_{CS}}$ profile for the current user. MVS/Express usernames are provided by DMV and added as part of the same process in which the Access IRP flag is updated.

Selection of this hyperlink transfers control to the MVS/Express web application. This web application allows a user to electronically submit applications for IRP credentials.

The transfer includes data about the current user. A process called "self-submitting forms" will be used to transfer both control and data to the web application. This process will take the current user's data from the $\mathrm{PORTAL_{CS}}$ database of users and encode it as an XML document. This information will be placed into a hidden field on a dynamically generated HTML page. The field name will be "baton."

The HTML page also will include the URL of a page within the MVS/Express web application. Once the HTML page has been created, the Portal will open this page. This will immediately and silently redirect a user to the specific URL in the web application. It will be the responsibility of MVS/Express to extract and parse the data in the hidden field.

Cambridge Systematics and ACS have agreed that the following format will be used to transfer control to MVS/Express, but note that the values shown are samples only:

```
<?xml version="1.0" encoding="UTF-8" ?>
<profileIRP>
  <returnURL>http://66.228.70.124/ct/receiveIRP.do</returnURL>
  <usernameIRP>MVSUSER</usernameIRP>
  <loginSequence>10615</loginSequence>
  <username>TESTCARRIER</username>
</profileIRP>
```

The MVS/Express web application provides a Logout function that returns control to the Portal Main Menu. When a user logs out of the MVS/Express system they are returned to the Portal. The web application will transfer data as part of the return process. Section A.2.3 provides further explanation.

### *Request IFTA Decals or Pay IFTA Taxes*

The Request IFTA Decals or Pay IFTA Taxes hyperlink appears only when the Access IFTA or Access RPC flags are set to Y for the current user in the PORTAL$_{CS}$ database of users. Also, if the current user is a carrier, as opposed to a service bureau, the carrier's IFTA status stored in the CVIEW$_{CS}$ database must be active for this hyperlink to be available. In order to check the carrier's IFTA status, the profile for the current user in the PORTAL$_{CS}$ database must include the carrier's IFTA account number. If this number is not available, the carrier's IFTA status cannot be checked and the carrier will be restricted to submitting only a new application.

Selection of this hyperlink transfers control to the IFTA$_{CS}$ credential web application. A user electronically submits applications for IFTA$_{CS}$ credentials through this web application, and from the web application can transfer a user to the RPC to pay IFTA taxes. The process by which control is transferred to the IFTA web application is described in Section 11.2.1 of the CI/CVIEW Detailed (Physical) Design. The process by which control is transferred to the RPC is described in Section 11.7 of the CI/CVIEW Detailed (Physical) Design.

### *Apply for an Oversize/Overweight Permit*

The Apply for an Oversize/Overweight Permit hyperlink appears only if the Access OS/OW flag is set to Y for the current user in the PORTAL$_{CS}$ database of users.

Selection of this hyperlink transfers control to the e-PASS web application. This web application allows a user to electronically submit applications for OS/OW permits.

This transfer includes data about the current user. Self-submitting forms will be used to transfer both control and data to the e-PASS web application. This process will take the current user's data from the PORTAL$_{CS}$ database of users and encode it as an XML document. The information will be placed into a hidden field named "baton" on a dynamically generated HTML page.

The HTML page also will include the URL of a page within the e-PASS application. Once the HTML page has been created, PORTAL$_{CS}$ will open this page. This will immediately and silently redirect a user to the specific URL in the web application. It will be the responsibility of e-PASS to extract and parse the data in the hidden field.

The format of the transferred data will be determined in consultation with the Award 3 vendor, in advance of the interim Release 1 software release.

The e-PASS web application provides a Logout function that returns control to the Portal Main Menu. When a user logs out of the e-PASS system they are returned to the Portal. The web application will transfer data as part of the return process. Section A.2.3 provides further explanation.

### *Help*

The Help hyperlink is available to all users. Selection of the hyperlink displays a consolidated Help Page for the credentialing system. This page includes a list of topics at the top of the page. Clicking a topic moves a user to an internal bookmark within the Help Page and will display information for the associated topic.

### *Edit My Account*

The Edit My Account hyperlink is enabled only if the Maintain Account flag is set to Y for the current user in the $\text{PORTAL}_{\text{CS}}$ database of users. Selection of this hyperlink transfers a user to a page where current registration information for the account is displayed.

All information associated with the account may be changed except the username and the FEIN/SSN. A user also has the option to change Mailing Address and/or Contact Address. A separate hyperlink is provided for changing the password. A user must supply the current password as well as the new password in order to complete the change.

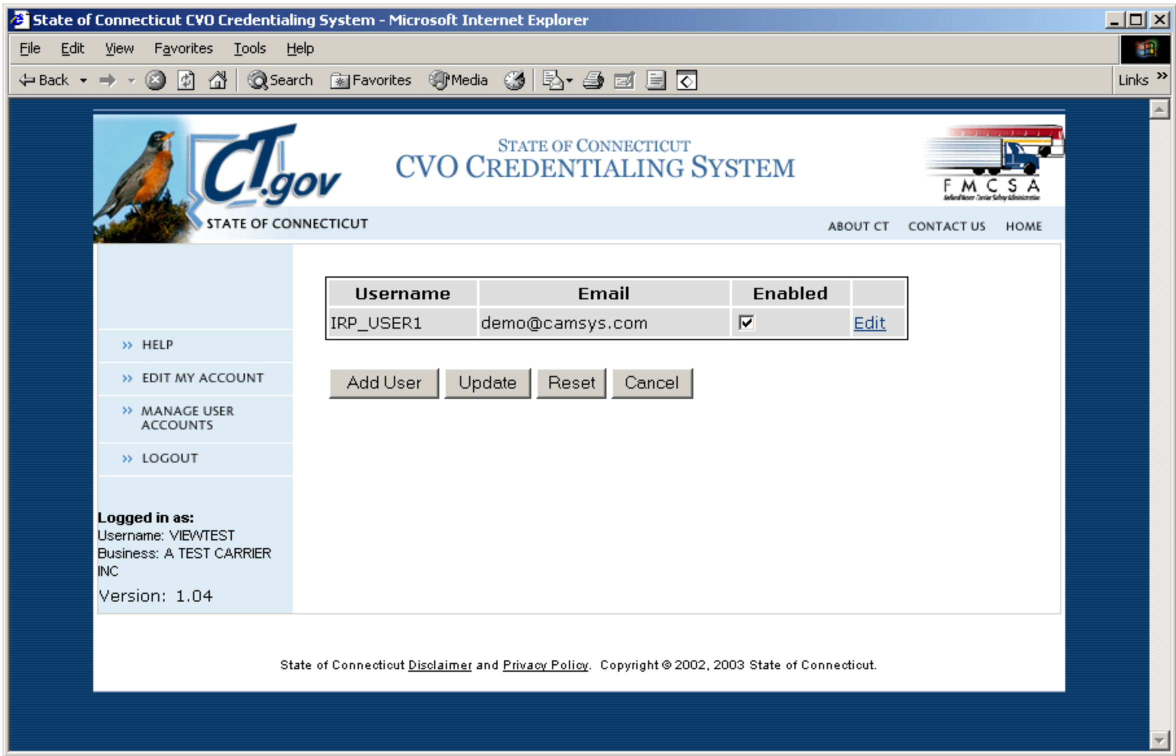
The page includes:

- Save button, which will update a user's registration information. This operation updates the existing profile in the Portal database and transfers control to the Portal Main Menu.
- Reset button, which will restore all information to its original state. This allows a user to start anew with the update.
- Cancel button, which will cancel the update and transfer control to the Portal Main Menu.
- Help hyperlink, which will open a separate browser window displaying a consolidated Help Page for the credentialing system.
- Manage User Accounts hyperlink, which will transfer control to the subaccount list window.
- Logout hyperlink, which will transfer control to the $\text{PORTAL}_{\text{CS}}$ Login Page.
- Home hyperlink, which will transfer control to the $\text{PORTAL}_{\text{CS}}$ Main Menu.

### *Manage User Accounts*

The Manage User Accounts hyperlink is enabled only if the Maintain Subaccounts flag is set to Y for the current user in the $\text{PORTAL}_{\text{CS}}$ database of users. Selection of this hyperlink transfers a user to the Manage User Accounts Page displaying the current list of subaccounts. A number of operations are available from this page. Figure A.10 illustrates the Manage User Accounts/Subaccount List. Figure A.11 illustrates the Update Subaccount Page. Figure A.12 illustrates the Add a Subaccount Page.

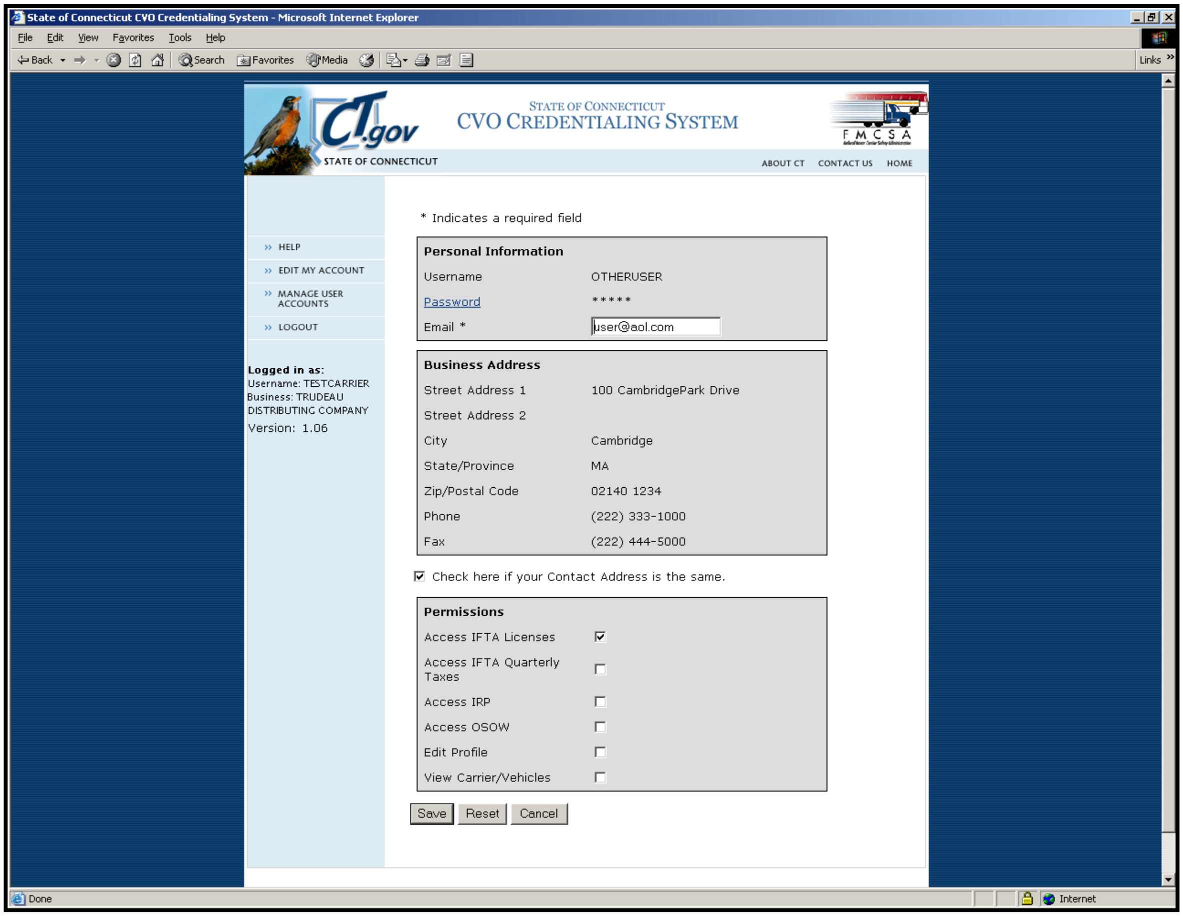
## Figure A.10 Manage User Accounts/Subaccount List



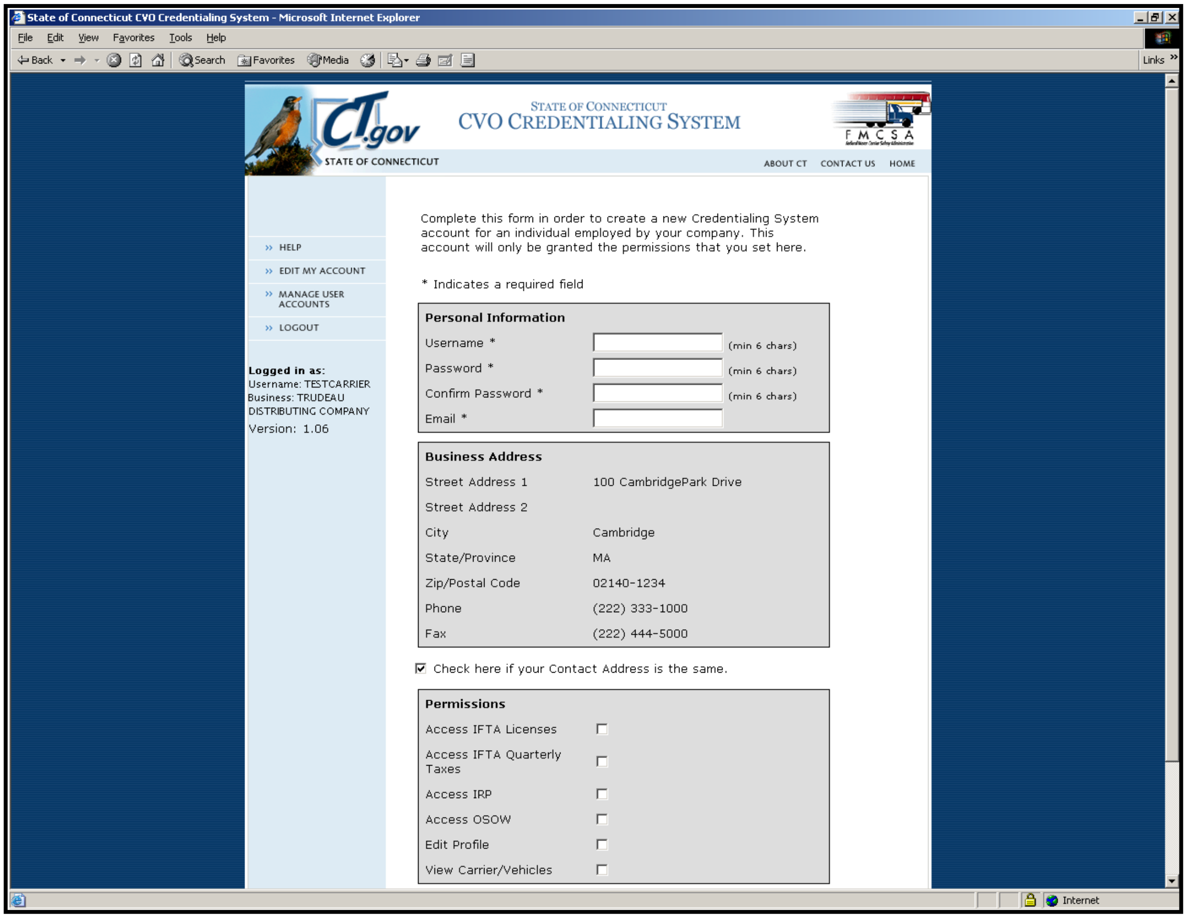

Clicking the Update button will apply a change to the Enabled checkbox next to a subaccount. Subaccounts are enabled by default when created. The master account may disable or enable a subaccount from the subaccount list window. The Enabled checkbox may be unchecked to disable the account or checked to enable the account. A user who is ready to submit the new status clicks the Update button. The operation is processed, resulting in an update of the existing profile in the Portal database. A user remains on the Manage User Accounts Page.

Clicking the Add User button will transfer a user to the subaccount entry window, or Subaccount Management Page, in order to create a new subaccount.

# Figure A.11 Update Subaccount Page



## Figure A.12 Add a Subaccount Page




Subaccount Management Page is similar to the self-registration page except that business-level information cannot be entered or changed. Personal information must be entered for the subaccount, including a unique username, a password, and an e-mail address. Business Address information unique to the subaccount may be entered, and permissions may be assigned to the subaccount. Only permissions that are available to the master account may be granted to the subaccount. However, the Master Account and Maintain Subaccounts flags cannot be set for a subaccount because they are reserved for master accounts.

The page includes:

- Add User button, which will create this subaccount with the assigned privileges. This operation results in a new profile written to the Portal database. A user is returned to the Manage User Accounts Page.

- Reset button, which will restore all information to its original state. This allows a user to start anew with the subaccount creation.

- Cancel button, which will return a user to the Manage User Accounts Page.

Clicking on the Edit hyperlink located next to each listed subaccount will transfer a user to the Subaccount Management Page with the current information for the subaccount already displayed. This information for the subaccount can be changed and updated.

The page includes:

- Save button, which will submit the updated information. This operation updates the existing profile in the Portal database. A user is returned to the Manage User Accounts Page.

- Reset button, which will restore all information to its original state. This allows a user to start anew with the update.

- Cancel button, which will return a user to the Manage User Accounts Page.

The Manage User Accounts Page also includes:

- Reset button that restores all information to its original state;

- Cancel button that returns a user to the Portal Main Menu;

- Help hyperlink that opens a separate browser window displaying a consolidated Help Page for the credentialing system;

- Edit My Account hyperlink that transfers a user to the Edit My Account Page; and

- Logout hyperlink that returns a user to the PORTAL$_{CS}$ Login Page.

- Home hyperlink, which will transfer control to the PORTAL$_{CS}$ Main Menu.

### *Logout*

The Logout hyperlink is available to all users. Selection of this hyperlink returns a user to the PORTAL$_{CS}$ Login Page. This operation updates a user login table (see Section A.4.6).

## A.2.3 Return to PORTAL$_{CS}$ Login Page

When a user completes operations in one of the web-based credential applications, the application will provide a way to return control to PORTAL$_{CS}$. The same self-submitting forms process described above will be used to transfer control back to the Portal.

Each web application will transfer back to PORTAL$_{CS}$ the same data that was provided by PORTAL$_{CS}$ during the initial hand-off of control. The Portal will use this information to reestablish users' sessions without requiring them to login again, should their Portal sessions have timed-out while they were working within another system. The URL to which the web application will transfer control will be included as one of the values originally sent to the web application.

## A.3 Page Design

The design of each PORTAL$_{CS}$ page is described below.

### *PORTAL$_{CS}$ Login Page*

This page is presented to a user who arrives at PORTAL$_{CS}$. This page provides fields for a user to enter his/her username and password. When a user clicks the Login button, the username and password will be matched with entries in the PORTAL$_{CS}$ database of users. Following a successful match, a user will be transferred to the PORTAL$_{CS}$ Main Menu. Username and login time/date will be recorded in the USER_LOGIN table.

A user may select the checkbox indicating that they are on a public computer. Selecting the checkbox will log them in with a higher security level, causing his/her session to time out sooner than at a lower security level.

The Login Page provides a number of additional user options:

- Help;
- Register as a Carrier;
- Register as a Service Bureau;
- Forgot Your Password?; and
- Home.

Clicking on the Help hyperlink opens the Help Page in a separate browser window. *This hyperlink also is located in the side bar of the self-registration and forgotten password pages.*

Clicking on the Register as a Carrier hyperlink opens the carrier self-registration page in the same browser window. *This hyperlink also is located in the side bar of the self-registration and forgotten password pages.*

Clicking on the Register as a Service Bureau hyperlink opens the service bureau self-registration page in the same browser window. *This hyperlink also is located in the side bar of the self-registration and forgotten password pages.*

Clicking on the Forgot Your Password? hyperlink opens the forgotten password page in the same browser window. *This hyperlink also is located in the side bar of the self-registration and forgotten password pages.*

A user who clicks on the Home hyperlink remains on the Login Page. *This hyperlink also is located in the upper right bar of the self-registration and forgotten password pages.* Clicking on this hyperlink on these pages returns a user to the Login Page.

### *Register as a Carrier Page*

The Register as a Carrier Page is presented when a user clicks on the Register as a Carrier hyperlink on the PORTAL$_{CS}$ Login Page. This page allows a user to enter all the information associated with establishing an account for submitting credential applications electronically.

The registration form consists of one data entry page. This page includes three blocks of fields: Personal Information, Business Information, and Business Address.

Personal Information contains the following fields, all of which are required:

- Username;
- Password;
- Confirm Password; and
- E-mail.

Business Information contains the following fields, with the required fields indicated:

- Company Name – required;
- Doing Business As;
- Tax ID (either FEIN or SSN) – required;
- U.S. DOT;
- IRP;
- IFTA; and
- Tax Registration Number – required *if* IFTA number is supplied.

Business Address contains the following fields, with the required fields indicated:

- Street Address 1 – required;
- Street Address 2;
- City – required;
- State/Province – required;

- Zip/Postal Code – required;
- Phone – required; and
- Fax.

At the bottom of the page are two check boxes for indicating whether Mailing Address and Contact Address are the same as Business Address. If a user unchecks a box, an additional block for entering information is displayed.

A user who has finished entering data may click the Register button to submit the registration form. In addition to verifying that a user enters all required elements, each element will be checked for data type and length (see Section A.5.2 for edit rules concerning this form).

If no errors are encountered, a user is returned to the Portal Login Page where they may log in using the username and password they entered. Note that the act of registering does not log in a user. If errors are encountered with the registration, the current page will be redisplayed with all data values intact and error message(s) shown at the top of the page. A user must correct the errors before his/her account can/will be updated.

The operation to Register as a Carrier writes the carrier's profile to the Portal database. See Section A.4 for details.

Two additional buttons are available on this page. Clicking the Reset button clears all fields of entered information and allows a user to start anew with the registration. Clicking the Cancel button cancels the registration and returns a user to the Portal Login Page.

### *Register as a Service Bureau Page*

The Register as a Service Bureau Page is presented when a user clicks on the Register as a Service Bureau hyperlink on the $\text{PORTAL}_{\text{CS}}$ Login Page. This page allows a user to enter all the information associated with establishing an account for submitting credential applications electronically.

The registration form consists of one data entry page. This page includes three blocks of fields: Personal Information, Business Information, and Business Address.

Personal Information contains the following fields, all of which are required:

- Username;
- Password;
- Confirm Password; and
- E-mail.

Business Information contains the following fields, with the required fields indicated:

- Company Name – required;
- Doing Business As; and
- Tax ID (either FEIN or SSN).

Business Address contains the following fields, with the required fields indicated:

- Street Address 1 – required;
- Street Address 2;
- City – required;
- State/Province – required;
- Zip/Postal Code – required;
- Phone – required; and
- Fax.

At the bottom of the page are two check boxes for indicating whether Mailing Address and Contact Address are the same as Business Address. By default, the boxes are presented to a user with checkmarks signifying that the addresses are the same. If a user unchecks a box, an additional block for entering information is displayed.

A user who has finished entering data may click the Register button to submit the registration form. In addition to verifying that a user enters all required elements, each element will be checked for data type and length (see Section A.5.3 for edit rules concerning this form).

If no errors are encountered, a user is returned to the Portal Login Page where they may log in using the username and password entered. Note that the act of registering does not log in a user. If errors are encountered with the registration, the current page will be redisplayed with all data values intact and error message(s) shown at the top of the page. A user must correct the errors before his/her account can/will be updated.

The operation to Register as a Service Bureau writes the service bureau's profile to the Portal database. See Section A.4 for details.

Two additional buttons are available on this page. Clicking the Reset button clears all fields of entered information and allows a user to start anew with the registration. Clicking the Cancel button cancels the registration and returns a user to the Portal Login Page.

### *Forgot Your Password? Page*

The Forgot Your Password? Page is presented when a user clicks on the Forgot Your Password? hyperlink on the $\text{PORTAL}_{\text{CS}}$ Login Page. This page allows a user who has forgotten his/her password to reset it. A user is prompted to enter his/her username and click the Submit button. This action resets the password for the account and sends it to the e-mail address that is associated with the username and stored in a user's profile.

This operation results in an entry in the Portal MESSAGE table (see Section A.4.3). This table is used to hold error and informational messages generated by the system.

Clicking the Submit button returns a user to the Portal Login Page. A user also has the option to click the Cancel button to cancel the operation and return to the Login Page.

### *Help Page (prior to logging in)*

The Help Page is presented when a user clicks on the Help hyperlink located in the side bar of the Login, Register as a Carrier, Register as a Service Bureau, and Forgot Your Password? Pages. This action opens in a separate browser window. This page provides detailed instructions for logging in, self-registration, and resetting one's password.

This page contains a list of topics at the top of the page that includes Register as a Carrier, Register as a Service Bureau, and Forgot Your Password?. Clicking a topic moves a user to an internal bookmark within the Help Page and will display information for the selected topic.

### *PORTAL$_{CS}$ Main Menu Page*

The Portal Main Menu is presented when a user has successfully logged in. This page welcomes a user to the State of Connecticut CVO Credentialing System, and presents a list of operations. The operations are adjusted dynamically based on security flags associated with users and stored in the PORTAL$_{CS}$ profiles. These security flags have default values according to agency business processes and whether a user is a carrier or a service bureau.

The dynamically adjusted list of operations includes the following:

- View Carrier and Vehicle Information;
- Update IRP Vehicle Registrations;
- Request IFTA Decals or Pay IFTA Taxes; and
- Apply for an Oversize/Overweight Permit.

Clicking on the View Carrier and Vehicle Information hyperlink opens the Carrier Snapshot Detail Page in the same browser window. This hyperlink appears only if the View Carrier Information flag is set to Y for the current user in the PORTAL$_{CS}$ database of users.

The Update IRP Vehicle Registrations hyperlink appears only if the Access IRP flag is set to Y for the current user in the PORTAL$_{CS}$ database of users and a non-blank MVS/Express username has been added to the PORTAL$_{CS}$ profile for the current user.

Clicking on this hyperlink transfers control from $PORTAL_{CS}$ to the MVS/Express web application. The transfer includes data about a user.

The Request IFTA Decals or Pay IFTA Taxes hyperlink appears only when the Access IFTA or Access RPC flags are set to Y for the current user in the $PORTAL_{CS}$ database of users. Also, if the current user is a carrier, as opposed to a service bureau, the carrier's IFTA status stored in the $CVIEW_{CS}$ database must be active for this hyperlink to be available. Clicking on this hyperlink transfers control from $PORTAL_{CS}$ to the $IFTA_{CS}$ credential web application. The transfer includes data about a user.

The Apply for an Oversize/Overweight Permit hyperlink appears only if the Access OS/OW flag is set to Y for the current user in the $PORTAL_{CS}$ database of users. Clicking on this hyperlink transfers control from $PORTAL_{CS}$ to the e-PASS web application. The transfer includes data about a user.

Additional user options include:

- Help;
- Edit My Account;
- Manage User Accounts;
- Logout; and
- Home.

Clicking on the Help hyperlink opens the Help Page in a separate browser window. *This hyperlink is located in the side bar of any page within the credentialing system.*

The Edit My Account hyperlink located in the side bar of multiple locations within the credentialing system is enabled only if the Maintain Account flag is set to Y for the current user in the $PORTAL_{CS}$ database of users. Clicking on this hyperlink opens a page in the same browser window where current registration information for the account is displayed.

The Manage User Accounts hyperlink located in the side bar of multiple locations within the credentialing system is enabled only if the Maintain Subaccounts flag is set to Y for the current user in the $PORTAL_{CS}$ database of users. Clicking on this hyperlink opens a page in the same browser window where the current list of subaccounts is displayed.

Clicking on the Logout hyperlink returns a user to the $PORTAL_{CS}$ Login Page. *This hyperlink is located in the side bar of any page within the credentialing system.*

Clicking on the Home hyperlink returns a user to the $PORTAL_{CS}$ Main Menu. *This hyperlink is located in the upper right bar of any page within the credentialing system.*

### *Help Page (within PORTAL$_{CS}$)*

The Help Page is presented when a user clicks on the Help hyperlink located in the side bar of all pages. It opens in a separate browser window. This page provides detailed instructions for completing the various credentialing and account management operations.

This page contains a list of topics at the top of the page that are broken down into Main CVO Credentialing System Menu and Side Bar Menu. The Main Menu includes the carrier/vehicle/permit snapshots and web applications for IFTA and IRP credentials and OS/OW permits. The Side Bar Menu includes the Edit My Account and Manage User Account functions. Clicking a topic moves a user to an internal bookmark within the Help Page and will display information for the selected topic.

### *Edit My Account Page*

The Edit My Account Page is presented when a user clicks on the Edit My Account hyperlink in the side bar. This page allows a user to update his/her registration information.

A user is presented with the registration form and the information stored in the Personal Information, Business Information, and Business Address fields with the exception of Password, which is concealed. All information except username and FEIN/SSN may be changed. A separate hyperlink is provided for changing the password. A user also has the option to change Mailing Address and/or Contact Address.

Personal Information contains the following fields:

- Username – cannot be changed;
- Password – required, concealed; and
- E-mail – required.

Business Information contains the following fields:

- Company Name – required;
- Doing Business As;
- FEIN or SSN – cannot be changed;
- U.S. DOT – not stored for service bureaus;
- IRP – not stored for service bureaus;
- IFTA – not stored for service bureaus; and
- Tax Registration Number – required *if* IFTA number is supplied (carriers), not stored for service bureaus.

Business Address contains the following fields:

- Street Address 1 – required;
- Street Address 2;
- City – required;
- State/Province – required;
- Zip/Postal Code – required;
- Phone – required; and
- Fax.

At the bottom of the page are two check boxes for indicating whether Mailing Address and Contact Address are the same as Business Address. By default, the boxes are presented to a user with checkmarks signifying that the addresses are the same. If a user unchecks a box, an additional block for entering information is displayed.

A user who has finished entering data may click the Save button to submit the updated registration information. In addition to verifying that a user enters all required elements, each element will be checked for data type and length (see Section A.5.5 for edit rules concerning this form).

If no errors are encountered, a user is returned to the Portal Main Menu. If errors are encountered, the current page will be redisplayed with all data values intact and error message(s) shown at the top of the page. A user must correct the errors before the registration form is accepted.

Clicking on the Password hyperlink on the Edit My Account Page opens the Change Password Page in the same browser window. Username is displayed. Values for Current Password, New Password, and Confirm New Password must be entered. A user who has finished entering data may click the Change button to change the password. A Cancel button also is available if a user elects not to change his/her password. Clicking either button returns a user to the Edit My Account Page.

Successful submittal of registration information, including a new password, updates the existing profile in the Portal database.

Two additional buttons are available on this page. Clicking the Reset button restores all information to its original state. Clicking the Cancel button cancels the update and returns a user to the Portal Main Menu.

### *Manage User Accounts and Subaccount Management Pages*

The Manage User Accounts Page is presented when a user clicks on the Manage User Accounts hyperlink in the side bar. This allows a user to perform operations on the subaccounts associated with a master account. The page lists the individual subaccounts including username, e-mail, and a box that if checked indicates that the subaccount is enabled as opposed to disabled.

The master account may disable or enable a subaccount from this page. The Enabled checkbox may be unchecked to disable the subaccount or checked to enable the subaccount. A user who is ready to submit a new status may click the Update button to process the operation. This operation updates the existing profile in the Portal database. A user remains on the Manage User Accounts Page.

Clicking the Add User button opens the Subaccount Management Page that displays a form for creating a new subaccount. Subaccounts inherit the business-level information of the master account (i.e., the Business Information and Business Address information). As a result, Business Information is not shown and Business Address is uneditable and shown for comparison purposes with Contact Address.

This page presents four blocks of fields: Personal Information, Business Address, Contact Address, and Permissions. As noted, Business Address fields are drawn from the master account and cannot be changed. Only permissions that are available to the master account may be granted to the subaccount.

Personal Information contains the following fields, all of which are required:

- Username;
- Password;
- Confirm Password; and
- E-mail.

Business Address contains the following fields, which are uneditable and all of them may not have values depending on whether the fields are required or not:

- Street Address 1;
- Street Address 2;
- City;
- State/Province;
- Zip/Postal Code;
- Phone; and
- Fax.

Contact Address fields are presented when a user arrives on the Subaccount Management Page. A user may check the box that says, "Check here if your Contact Address is the same" (as Business Address) and the Contact Address block will be eliminated from the page. The fields include:

- Street Address 1;
- Street Address 2;
- City;

- State/Province;
- Zip/Postal Code;
- Phone; and
- Fax.

The last block is the Permissions that will be granted to the subaccount from among the following:

- IFTA Access;
- RPC Access;
- IRP Access;
- OSOW Access;
- Edit Profile; and
- View Carrier.

A user who has completed the form may click the Add User button to create this subaccount with the assigned privileges. In addition to verifying that a user enters all required elements, each element will be checked for data type and length (see Section A.5.9 for edit rules concerning this form).

If no errors are encountered, a user is returned to the Manage User Accounts Page. If errors are encountered, the current page will be redisplayed with all data values intact and error message(s) shown at the top of the page. A user must correct the errors before the update is accepted.

This operation results in a new profile written to the Portal database.

Clicking on the Edit hyperlink located next to each listed subaccount opens the Subaccount Management Page with the current information for the subaccount already displayed for a user to edit. This page simply displays stored Personal Information, Business Address, Permissions, and Contact Address (if appropriate), with the exception of Password, which is concealed. Username and Business Address fields cannot be changed. A separate hyperlink is provided for changing the Password (see details under Edit My Account Page immediately above).

The following fields are shown:

- Personal Information – Username, Password (required), and E-mail (required);
- Business Address (no fields can be changed) – Street Address 1, Street Address 2, City, State/Province, Zip/Postal Code, Phone, and Fax; and
- Permissions – IFTA Access, RPC Access, IRP Access, OSOW Access, Edit Profile, and View Carrier.

In the middle of the page following the Business Address block is a check box to indicate whether Contact Address is the same as Business Address. A checkmark signifies the same address. A user may check or uncheck the box as necessary. A user who wishes to enter Contact Address information is presented with an additional block for entering this information.

A user who has finished entering data may click the Save button to submit the update. In addition to verifying that a user enters all required elements, each element will be checked for data type and length (see Section A.5.8 for edit rules concerning this data).

If no errors are encountered, a user is returned to the Manage User Accounts Page. If errors are encountered, the current page will be redisplayed with all data values intact and error message(s) shown at the top of the page. A user must correct the errors before the update is accepted.

This operation updates the existing profile in the Portal database.

Two additional buttons are available to a user who arrives on the Subaccount Management Page, whether to add a subaccount or edit a subaccount. Clicking the Reset button clears all fields of entered information and allows a user to start anew with the subaccount creation or update. Clicking the Cancel button cancels the operation and returns a user to the Manage User Accounts Page.

### *View Carrier and Vehicle Information Pages*

The Carrier Snapshot Detail Page is presented when a carrier user clicks on the View Carrier and Vehicle Information hyperlink on the $\text{PORTAL}_{\text{CS}}$ Main Menu Page. The snapshot for an individual carrier is retrieved based on the FEIN/SSN stored in carrier's $\text{PORTAL}_{\text{CS}}$ profile. A State user who selects this hyperlink is first presented with an intermediate page [Carrier Selection Page described in Sections 11.2.2 and 11.3.2 of the CI/CVIEW Detailed (Physical) Design] that requests carrier identifying information such as U.S. DOT number, FEIN, or SSN. Once the carrier snapshot has been successfully located in the $\text{CVIEW}_{\text{CS}}$ database, the Carrier Snapshot Detail Page for that carrier is displayed. Service bureau users will not be allowed to view carrier snapshots unless the carrier provides them with subaccount information from the carrier's master account.

The Carrier Snapshot Detail Page is the first in a series of pages that display carrier, vehicle, and permit information. Additional pages include:

- Vehicle List Page;
- Vehicle Snapshot Detail Page;
- Permit List Page; and
- Permit Detail Page.

The Carrier Snapshot Detail Page displays data for one carrier drawn from the Connecticut $\text{CVIEW}_{\text{CS}}$ database. The page contains the following information.

- Carrier Information – Carrier Name; DBA Name; U.S. DOT Number; Tax ID Type and Number; Telephone Number; Fax Number; E-mail Address; ISS Score and Score Date; SafeStat Score and Date; MCSIP Flag, Level, and Level Date; and OOS Report Number, Date, Reason, and Status;

- Carrier Addresses – Business, Mailing, and Physical;

- IFTA Information – License Number, Base State, Status, Status Date, Issue Date, and Expire Date; and

- IRP Information – Carrier Fleet, Account Number, State of Registration, Status, Status Date, Issue Date, Expire Date, and Comment.

OS/OW permit information will be added to the Carrier Snapshot Detail Page, if appropriate, as part of the interim Release 1.

Individual fields without data values will display as blank. If no IRP data are available for a carrier, the carrier snapshot will display the "IRP Information" title and the message "No information" will be displayed instead of the IRP information box. If no IFTA data are available for the carrier, the carrier snapshot will display the "IFTA Information" title and the message "No information" will be displayed instead of the IFTA information box.

Clicking on the View Carrier's Vehicle List hyperlink on the Carrier Snapshot Detail Page opens the Vehicle List Page for this carrier. This page displays a list of vehicles associated with this carrier. Only vehicles for which a relationship with the carrier has been identified (i.e., through information supplied by the IRP system, transponder registration system, or PRISM Target File) will be reported. If no vehicles are found for the carrier, $\text{PORTAL}_{\text{CS}}$ will display the message "Sorry, no vehicles found for this carrier!"

For each vehicle, the Vehicle List Page displays License State, License Number, and VIN. Each record in the list has a hyperlink to the Vehicle Snapshot Detail Page for the specified vehicle. There is no circumstance in which a selected vehicle snapshot will not be found once a vehicle is selected on the Vehicle List Page.

Clicking on the Detail hyperlink on the Vehicle List Page opens the Vehicle Snapshot Detail Page. This page displays data for one vehicle drawn from the Connecticut $\text{CVIEW}_{\text{CS}}$ database. The page contains the following information:

- Vehicle Information – VIN, Unit Number, Title Number and Jurisdiction, Transponder Number, Model Year, Make, Type, Model, Fuel, Unladen Weight, Number of Axles, Number of Seats, Owner Name, Primary color, and Secondary color;

- Registration Information – License Plate Country, State, and Number; State of Registration; IRP Account Number, Fleet Number, and Status; Start Date and Expire Date; and Registered Gross Vehicle Weight; and

- IRP Jurisdictions – List of IRP jurisdictions and registered weights for the vehicle, including the QUAL indicator for each jurisdiction.

Individual fields without data values will display as blank.

As part of interim Release 1, the Vehicle Snapshot Detail Page will be updated to contain a hyperlink to the Permit List for this vehicle. Clicking on the Permit List hyperlink for the vehicle will open the Permit List Page. This page will display a list of oversize/overweight permits, if any, associated with this vehicle.

For each permit on the Permit List Page, the Permit Number, Permit Start Date, and Permit Expire Date likely will be displayed. Each record in the list will be a hyperlink to the Permit Detail Page for the specified permit.

(Note: The exact content to be displayed will be determined as part of the OS/OW design effort for interim Release 1. This page will be implemented as part of interim Release 1.)

Clicking on the Permit Detail hyperlink on the Permit List Page will open the Permit Detail Page. This page will display data for one oversize/overweight permit drawn from the Connecticut $\text{CVIEW}_{\text{CS}}$ database. The page will contain the following information:

- Permit Information;
- Axle Weights and Spacings; and
- Restrictions.

(Note: The exact content to be displayed will be determined as part of the OS/OW design effort for interim Release 1. This page will be implemented as part of interim Release 1.)

The sidebar on the carrier, vehicle, and permit pages will include the following operations:

- Clicking on the Help hyperlink opens a separate browser window displaying a consolidated Help Page for the credentialing system.
- Clicking on the SAFER Snapshot hyperlink transfers a user to the SAFER web site for information on the current carrier.
- Clicking on the SafeStat Snapshot hyperlink transfers a user to the SafeStat web site for information on the current carrier.
- Clicking on the Logout hyperlink returns a user to the $\text{PORTAL}_{\text{CS}}$ Login Page.

In addition, a Home hyperlink is available in the upper right bar of these pages. Clicking on this hyperlink returns a user to the $\text{PORTAL}_{\text{CS}}$ Main Menu.

# A.4 Data Design

The PORTAL$_{CS}$ database has a single schema called PORTAL that supports Portal operations including user authentication, logging of exception conditions and other significant actions, and logging of electronic payment operations. The schema contains the following information:

- Profiles of registered users, including username, password, permissions associated with a user, business-level information (firm name, DBA, FEIN, credential account numbers, etc.), and address and contact information;
- Specific instances of a user logging in and logging out of the Portal;
- Error log and other recorded events; and
- Log of electronic payment operations.

This information is stored in the following tables within the PORTAL schema:

- ADDRESS table;
- BUSINESS table;
- MESSAGE table;
- PAYMENT table;
- USERS table; and
- USER_LOGIN table.

## A.4.1 ADDRESS Table

The ADDRESS table contains the address-related information for the various accounts.

| | |
|---|---|
| Name: | ADDRESS |
| Primary Key: | PK_ADDRESS |
| Comment: | This entity contains the address related information for the various accounts. |

Table A.1 describes the table columns. Records are inserted into the table during the PORTAL$_{CS}$ self-registration process and when a master account creates subaccounts.

## Table A.1 ADDRESS Table Columns

| Name | Data Type | Comment | Primary | Mandatory |
|---|---|---|---|---|
| ADDRESSTYPE | VARCHAR2(10) | Type of address. Valid values are “physical,” “mailing” and “contact” | X | X |
| OWNERTYPE | VARCHAR2(10) | Type of owner. Valid values are “firm” or “user” | X | X |
| OWNERID | VARCHAR2(20) | Foreign key into either the BUSINESS or USERS table depending on OWNERTYPE | X | X |
| NAME | VARCHAR2(40) | NAME | | |
| STREET | VARCHAR2(40) | Street address | | |
| CITY | VARCHAR2(30) | City doing business in | | |
| STATE | VARCHAR2(6) | Jurisdiction doing business in | | |
| ZIP | VARCHAR2(10) | Postal code. Can handle both the US 5-digit+4 and the Canadian 6 alphanumeric forms | | |
| PHONE | VARCHAR2(12) | The telephone number at the principal place of business | | |
| FAX | VARCHAR2(12) | The fax number at the principal place of business. | | |

### A.4.2 BUSINESS Table

The BUSINESS table contains information related to the businesses (i.e., carrier, service bureau, or State) that have accounts.

| | |
|---|---|
| Name: | BUSINESS |
| Primary Key: | PK_BUSINESS |
| Comment: | Information related to the businesses that have accounts. In this context a business is either a carrier, service bureau or the state |

Table A.2 describes the table columns. Records are inserted into the table during the $PORTAL_{CS}$ self-registration process and when a master account creates subaccounts.

## Table A.2 BUSINESS Table Columns

| Name | Data Type | Comment | Primary | Mandatory |
|---|---|---|---|---|
| DBID | VARCHAR2(20) | Internally generated database sequence number | X | X |
| FIRMTYPE | VARCHAR2(10) | Type of company. Valid values are "carrier," "service" or "state" | | |
| FIRMNAME | VARCHAR2(55) | This is the legal name of the firm May include organization name or first, middle and last name of a person. | | |
| NAMEDBA | VARCHAR2(55) | Doing Business As name. This may be a trade name under which the firm does business. Any name identifying the entity other than the legal name. | | |
| TAXID | VARCHAR2(12) | Either the FEIN or SSN depending on Y4SSN | | |
| Y4SSN | CHAR | TAXID type. Y=social security number, anything else=FEIN | | |
| USDOT | VARCHAR2(12) | US Dept. of Transportation ID number | | |
| IFTA | VARCHAR2(18) | IFTA account number | | |
| IRP | VARCHAR2(18) | IRP account number | | |
| OSOW | VARCHAR2(18) | OSOW account number | | |
| RPC | VARCHAR2(18) | IFTA RPC account number | | |
| TAXREGNUM | VARCHAR2(12) | Carrier tax registration number | | |

### A.4.3 MESSAGE Table

The MESSAGE table contains informational or error messages that are generated. Records are generated by exception conditions and other significant actions within the Portal and inserted into the table.

| | |
|---|---|
| Name: | MESSAGE |
| Primary Key: | PK_MESSAGE |
| Comment: | Repository for any informational or error messages that are generated |

Table A.3 describes the table columns.

### Table A.3 MESSAGE Table Columns

| Name | Data Type | Comment | Primary | Mandatory |
|---|---|---|---|---|
| MESSAGEID | NUMBER(15) | Internally generated database sequence number | X | X |
| LOGINSEQUENCE | NUMBER(15) | Foreign key into the PORTAL.USER_LOGIN table | | |
| USERNAME | VARCHAR2(20) | Login username | | |
| TIMESTAMP | DATE | Date/time the message was generated | | |
| MESSAGETYPE | CHAR | Type of message generated. Valid values are "I"=informational, "E"=error | | |
| MESSAGE | CLOB | The content of the message | | |

## A.4.4 PAYMENT Table

The PAYMENT table contains electronic payment transactions and their results. Records of input information provided by the credential web applications, and reference numbers and results of transactions from the e-payment vendor, are inserted into the table.

| | |
|---|---|
| Name: | PAYMENT |
| Primary Key: | PK_PAYMENT |
| Comment: | Electronic payment transactions and their results |

Table A.4 describes the table columns.

## Table A.4 PAYMENT Table Columns

| Name | Data Type | Comment | Primary | Mandatory |
|---|---|---|---|---|
| PAYMENTID | NUMBER(15) | Internally generated database sequence number | X | X |
| TRANSACTIONID | NUMBER(15) | Transaction sequence number from the IFTA data model TRANSACTION table | | X |
| AGENCYNAME | VARCHAR2(55) | Name of the state agency for whom the payment is due. Valid values are "DMV," "DRS" and "DOT" | | |
| CREDENTIAL | VARCHAR2(55) | Description of credential to be purchased | | |
| USERNAME | VARCHAR2(20) | Foreign key into the USERS table that indicates who is doing the purchasing | | |
| CARRIERNAME | VARCHAR2(55) | Name of the carrier for whom the credential is being purchased | | |
| AMOUNT | NUMBER(10,2) | Total amount due | | |
| SALESTAX | NUMBER(10,2) | Sales tax due. This amount is included in the AMOUNTDUE | | |
| PAYMENTREFERENCE NUMBER | VARCHAR2(30) | Reference number provided by VeriSign | | |
| PAYMENTRESULT CODE | VARCHAR2(2) | Result code. Valid values are 0=transaction was approved, anything else=error | | |
| PAYMENTRESULTMSG | CLOB | Message associated with the result code | | |

### A.4.5 USERS Table

The USERS table contains information about each user that allows them to login to the Portal and determines the functions they can perform.

| | |
|---|---|
| Name: | USERS |
| Primary Key: | PK_USER |
| Comment: | Information for each user that allows them to logon and determine what functions they can perform |

Table A.5 describes the table columns. Records are inserted into the table during the $PORTAL_{CS}$ self-registration process and when a master account creates subaccounts.

## Table A.5 USERS Table Columns

| Name | Data Type | Comment | Primary | Mandatory |
|---|---|---|---|---|
| PERMISSIONS | CHAR(10) | Series of Ys or Ns of the permissions associated with the user. Valid permissions are Enabled, Master, Maintain_Self, Maintain_Subs, View_Carrier, Access_IFTA, Access_IRP, Access_OSOW, Access_RPC | | |
| USERNAME | VARCHAR2(20) | Login username | X | X |
| PASSWORD | VARCHAR2(20) | Login password | | |
| EMAIL | VARCHAR2(256) | e-mail address associated with the user | | |
| IRPNAME | VARCHAR2(30) | User name needed to log into the MVS/Express IRP system | | |
| FIRMID | VARCHAR2(20) | Foreign key into the BUSINESS table | | |

## A.4.6 USER_LOGIN Table

The USER_LOGIN table contains records of the login and logout activity of each user. Records are generated by a user's instances of logging in and logging out.

| | |
|---|---|
| Name: | USERS |
| DBMS: | ORACLE Version 9i |
| Primary Key: | PK_U_LOGIN |
| Comment: | This table is used to record the login/logout activity of each user |

Table A.6 describes the table columns.

### Table A.6 USER_LOGIN Table Columns

| Name | Data Type | Comment | Primary | Mandatory |
|---|---|---|---|---|
| LOGINSEQUENCE | VARCHAR2(20) | Internally generated database sequence number | X | X |
| USERNAME | VARCHAR2(20) | Foreign key into either the USERS table | | X |
| LOGINTIME | DATE | Date/time the user logged in | | |
| LOGOUTTIME | DATE | Date/time the user logged out | | |

## A.5 Edit Rules

### Table A.7 Login Page

| Field Name | Data Type | Length | Required | Default Value | Location | Comments |
|---|---|---|---|---|---|---|
| Username | AN | 20 | Yes | No | Page 1 | Minimum of six characters including alphanumeric, under-score, hyphen, and period. Data entered is checked against user's $PORTAL_{CS}$ profile |
| Password | AN | 20 | Yes | No | Page 1 | Minimum of six characters including alphanumeric, under-score, hyphen, and period. Data entered is checked against user's $PORTAL_{CS}$ profile |
| Using a Public Computer | N/A | N/A | No | Not Using a Public Computer (unchecked box) | Page 1 | Check in box indicates use of a public computer, and lowers session timeout to 10 minutes |

## Table A.8 Register as a Carrier Page

| Field Name | Data Type | Length | Required | Default Value | Location | Comments |
|---|---|---|---|---|---|---|
| Username | AN | 20 | Yes | No | Page 1 | Minimum of six characters, including alphanumeric, under-score, hyphen, and period |
| Password | AN | 20 | Yes | No | Page 1 | Minimum of six characters, including alphanumeric, under-score, hyphen, and period |
| Confirm Password | AN | 20 | Yes | No | Page 1 | Value must equal "Password" |
| E-mail | AN | See Comment | Yes | No | Page 1 | Must match form of a valid e-mail address |
| Company Name | AN | 55 | Yes | No | Page 1 | |
| Doing Business As | AN | 55 | No | No | Page 1 | Name if different from "Company Name" |
| Tax ID | (A)<br>N | (N/A)<br>9<br>See Comment | Yes | No | Page 1 | (A) is one from drop-down list of "FEIN" and "SSN." Either FEIN or SSN is N=9. If FEIN, [1-2][3-9] = "xx""xxxxxxx." If SSN, [1-3][4-5][6-9] = "xxx""xx""xxxx." Formula is used to check for valid SSN |
| U.S. DOT | N | 6<br>See Comment | No | No | Page 1 | Length could be 6–8 |
| IRP | N | 6 | No | No | Page 1 | |
| IFTA | AN | 13 | No | No | Page 1 | "CTxxxxxxxxxnn" where xxxxxxxxx = FEIN or SSN |
| Tax Reg. Num. | N | 10<br>[1-7]<br>[8-10] | No*<br>See Comment | No | Page 1 | "xxxxxxx""xxx." Registration with Connecticut Department of Revenue Services. Required if IFTA number is supplied |
| Business Street Address 1 | AN | 40 | Yes | No | Page 1 | |
| Business Street Address 2 | AN | 40 | No | No | Page 1 | |
| Business City | AN | 30 | Yes | No | Page 1 | |
| Business State/Province | A | N/A | Yes | No | Page 1 | One from drop-down list of U.S. states, District of Columbia, Canada provinces and territories |
| Business Zip/Postal Code | AN | 10<br>[1-6]<br>[7-10] | Yes | No | Page 1 | If U.S., minimum "xxxxx." If Canada, "xnxnxn" |
| Business Phone | N | 10<br>[1-3]<br>[4-6]<br>[7-10] | Yes | No | Page 1 | Three-digit area code and seven-digit phone number (no punctua-tion marks) |

# Table A.8 Register as a Carrier Page (continued)

| Field Name | Data Type | Length | Required | Default Value | Location | Comments |
|---|---|---|---|---|---|---|
| Business Fax | N | 10<br>[1-3]<br>[4-6]<br>[7-10] | No | No | Page 1 | Three-digit area code and seven-digit phone number (no punctuation marks) |
| Mailing Street Address 1 | AN | 40 | No | No | Page 1 | If "Mailing Address" differs from "Business Address," "Mailing Address" box is unchecked to display additional set of address fields for entering data |
| Mailing Street Address 2 | AN | 40 | No | No | Page 1 | |
| Mailing City | AN | 30 | No | No | Page 1 | |
| Mailing State/Province | A | N/A | No | No | Page 1 | No more than one from drop-down list of U.S. states, District of Columbia, Canada provinces and territories |
| Mailing Zip/Postal Code | AN | 10<br>[1-6]<br>[7-10] | No | No | Page 1 | If U.S., "xxxxx"("xxxx"). If Canada, "xnxnxn" |
| Contact Street Address 1 | AN | 40 | No | No | Page 1 | If "Contact Address" differs from "Business Address," "Contact Address" box is unchecked to display additional set of address and phone fields for entering data |
| Contact Street Address 2 | AN | 40 | No | No | Page 1 | |
| Contact City | AN | 30 | No | No | Page 1 | |
| Contact State/Province | A | N/A | No | No | Page 1 | No more than one from drop-down list of U.S. states, District of Columbia, Canada provinces and territories |
| Contact Zip/Postal Code | AN | 10<br>[1-6]<br>[7-10] | No | No | Page 1 | If U.S., "xxxxx"("xxxx"). If Canada, "xnxnxn" |
| Contact Phone | N | 10<br>[1-3]<br>[4-6]<br>[7-10] | No | No | Page 1 | Three-digit area code and seven-digit phone number (no punctuation marks) |
| Contact Fax | N | 10<br>[1-3]<br>[4-6]<br>[7-10] | No | No | Page 1 | Three-digit area code and seven-digit phone number (no punctuation marks) |

# Table A.9 Register as a Service Bureau Page

| Field Name | Data Type | Length | Required | Default Value | Location | Comments |
|---|---|---|---|---|---|---|
| Username | AN | 20 | Yes | No | Page 1 | Minimum of six characters, including alphanumeric, underscore, hyphen, and period |
| Password | AN | 20 | Yes | No | Page 1 | Minimum of six characters, including alphanumeric, underscore, hyphen, and period |
| Confirm Password | AN | 20 | Yes | No | Page 1 | Value must equal "Password" |
| E-mail | AN | See Comment | Yes | No | Page 1 | Must match form of a valid e-mail address |
| Company Name | AN | 55 | Yes | No | Page 1 | |
| Doing Business As | AN | 55 | No | No | Page 1 | Name if different from "Company Name" |
| Tax ID | (A)<br>N | (N/A)<br>9<br>See Comment | No | No | Page 1 | (A) is one from drop-down list of "FEIN" and "SSN." Either FEIN or SSN is N=9. If FEIN, [1-2][3-9] = "xx""xxxxxxx." If SSN, [1-3][4-5][6-9] = "xxx""xx""xxxx." Formula is used to check for valid SSN |
| Business Street Address 1 | AN | 40 | Yes | No | Page 1 | |
| Business Street Address 2 | AN | 40 | No | No | Page 1 | |
| Business City | AN | 30 | Yes | No | Page 1 | |
| Business State/Province | A | N/A | Yes | No | Page 1 | One from drop-down list of U.S. states, District of Columbia, Canada provinces and territories |
| Business Zip/Postal Code | AN | 10<br>[1-6]<br>[7-10] | Yes | No | Page 1 | If U.S., minimum "xxxxx." If Canada, "xnxnxn" |
| Business Phone | N | 10<br>[1-3]<br>[4-6]<br>[7-10] | Yes | No | Page 1 | Three-digit area code and seven-digit phone number (no punctuation marks) |
| Business Fax | N | 10<br>[1-3]<br>[4-6]<br>[7-10] | No | No | Page 1 | Three-digit area code and seven-digit phone number (no punctuation marks) |
| Mailing Street Address 1 | AN | 40 | No | No | Page 1 | If "Mailing Address" differs from "Business Address," "Mailing Address" box is unchecked to display additional set of address fields for entering data |

## Table A.9 Register as a Service Bureau Page (continued)

| Field Name | Data Type | Length | Required | Default Value | Location | Comments |
|---|---|---|---|---|---|---|
| Mailing Street Address 2 | AN | 40 | No | No | Page 1 | |
| Mailing City | AN | 30 | No | No | Page 1 | |
| Mailing State/Province | A | N/A | No | No | Page 1 | No more than one from drop-down list of U.S. states, District of Columbia, Canada provinces and territories |
| Mailing Zip/Postal Code | AN | 10 [1-6] [7-10] | No | No | Page 1 | If U.S., “xxxxx”(“xxxx”). If Canada, “xnxnxn” |
| Contact Street Address 1 | AN | 40 | No | No | Page 1 | If “Contact Address” differs from “Business Address,” “Contact Address” box is unchecked to display additional set of address and phone fields for entering data |
| Contact Street Address 2 | AN | 40 | No | No | Page 1 | |
| Contact City | AN | 30 | No | No | Page 1 | |
| Contact State/Province | A | N/A | No | No | Page 1 | No more than one from drop-down list of U.S. states, District of Columbia, Canada provinces and territories |
| Contact Zip/Postal Code | AN | 10 [1-6] [7-10] | No | No | Page 1 | If U.S., “xxxxx”(“xxxx”). If Canada, “xnxnxn” |
| Contact Phone | N | 10 [1-3] [4-6] [7-10] | No | No | Page 1 | Three-digit area code and seven-digit phone number (no punctuation marks) |
| Contact Fax | N | 10 [1-3] [4-6] [7-10] | No | No | Page 1 | Three-digit area code and seven-digit phone number (no punctuation marks) |

## Table A.10 Forgot Your Password? Page

| Field Name | Data Type | Length | Required | Default Value | Location | Comments |
|---|---|---|---|---|---|---|
| Username | AN | 20 | No* See Comment | No | Page 1 | Required if password is to be e-mailed to user. Data entered is checked against user's $\text{PORTAL}_{\text{CS}}$ profile |

## Table A.11 Edit My Account Page

| Field Name | Data Type | Length | Required | Default Value | Location | Comments |
|---|---|---|---|---|---|---|
| Password | AN | 20 | Yes* See Comment | Yes* See note following table | Page 1 | Concealed; to change, click on "Password" hyperlink to display Change Password Page (Sec. A.5.6) |
| E-mail | AN | See Comment | Yes | Yes | Page 1 | Must match form of a valid e-mail address |
| Company Name | AN | 55 | Yes | Yes | Page 1 | |
| Doing Business As | AN | 55 | No | Yes | Page 1 | Name if different from "Company Name" |
| Tax ID | (A) N | (N/A) 9 See Comment | No | No | Page 1 | For service bureaus only. (A) is one from drop-down list of "FEIN" and "SSN." Either FEIN or SSN is N=9. If FEIN, [1-2][3-9] = "xx""xxxxxxx." If SSN, [1-3][4-5][6-9] = "xxx""xx""xxxx." Formula is used to check for valid SSN. Data saved is uneditable |
| U.S. DOT | N | 6 See Comment | No | Yes | Page 1 | Length could be 6–8. Not stored for service bureaus |
| IRP | N | 6 | No | Yes | Page 1 | Not stored for service bureaus |
| IFTA | AN | 13 | No | Yes | Page 1 | "CTxxxxxxxxxnn" where xxxxxxxxx = FEIN or SSN. Not stored for service bureaus |
| Tax Reg. Num. | N | 10 [1-7] [8-10] | No* See Comment | Yes | Page 1 | "xxxxxxx""xxx." Registration with Connecticut Department of Revenue Services. Required if IFTA number is supplied. Not stored for service bureaus |

## Table A.11 Edit My Account Page (continued)

| Field Name | Data Type | Length | Required | Default Value | Location | Comments |
|---|---|---|---|---|---|---|
| Business Street Address 1 | AN | 40 | Yes | Yes | Page 1 | |
| Business Street Address 2 | AN | 40 | No | Yes | Page 1 | |
| Business City | AN | 30 | Yes | Yes | Page 1 | |
| Business State/Province | A | N/A | Yes | Yes | Page 1 | One from drop-down list of U.S. states, District of Columbia, Canada provinces and territories |
| Business Zip/Postal Code | AN | 10 [1-6] [7-10] | Yes | Yes | Page 1 | If U.S., minimum "xxxxx." If Canada, "xnxnxn" |
| Business Phone | N | 10 [1-3] [4-6] [7-10] | Yes | Yes | Page 1 | Three-digit area code and seven-digit phone number (no punctuation marks) |
| Business Fax | N | 10 [1-3] [4-6] [7-10] | No | Yes | Page 1 | Three-digit area code and seven-digit phone number (no punctuation marks) |
| Mailing Street Address 1 | AN | 40 | No | Yes | Page 1 | If "Mailing Address" differs from "Business Address," "Mailing Address" box is unchecked to display additional set of address fields for entering data |
| Mailing Street Address 2 | AN | 40 | No | Yes | Page 1 | |
| Mailing City | AN | 30 | No | Yes | Page 1 | |
| Mailing State/Province | A | N/A | No | Yes | Page 1 | No more than one from drop-down list of U.S. states, District of Columbia, Canada provinces and territories |
| Mailing Zip/Postal Code | AN | 10 [1-6] [7-10] | No | Yes | Page 1 | If U.S., "xxxxx"("xxxx"). If Canada, "xnxnxn" |
| Contact Street Address 1 | AN | 40 | No | Yes | Page 1 | If "Contact Address" differs from "Business Address," "Contact Address" box is unchecked to display additional set of address and phone fields for entering data |
| Contact Street Address 2 | AN | 40 | No | Yes | Page 1 | |
| Contact City | AN | 30 | No | Yes | Page 1 | |

## Table A.11 Edit My Account Page (continued)

| Field Name | Data Type | Length | Required | Default Value | Location | Comments |
|---|---|---|---|---|---|---|
| Contact State/Province | A | N/A | No | Yes | Page 1 | No more than one from drop-down list of U.S. states, District of Columbia, Canada provinces and territories |
| Contact Zip/Postal Code | AN | 10<br>[1-6]<br>[7-10] | No | Yes | Page 1 | If U.S., "xxxxx"("xxxx"). If Canada, "xnxnxn" |
| Contact Phone | N | 10<br>[1-3]<br>[4-6]<br>[7-10] | No | Yes | Page 1 | Three-digit area code and seven-digit phone number (no punctuation marks) |
| Contact Fax | N | 10<br>[1-3]<br>[4-6]<br>[7-10] | No | Yes | Page 1 | Three-digit area code and seven-digit phone number (no punctuation marks) |

Note: *Yes indicates that a default value may be drawn from the PORTAL$_{CS}$ profile of the user.

## Table A.12 Change Password Page

| Field Name | Data Type | Length | Required | Default Value | Location | Comments |
|---|---|---|---|---|---|---|
| Password | AN | 20 | Yes | No | Page 2 | Current password |
| New Password | AN | 20 | Yes | No | Page 2 | Minimum of six characters, including alphanumeric, underscore, hyphen, and period |
| Confirm New Password | AN | 20 | Yes | No | Page 2 | Value must equal "New Password" |

## Table A.13 Manage User Accounts Page

| Field Name | Data Type | Length | Required | Default Value | Location | Comments |
|---|---|---|---|---|---|---|
| Enabled | N/A | N/A | See Comment | Enabled (checked box) | Page 1 | Removal of check from box disables account, i.e., prevents user from logging in; addition of check enables account |

## Table A.14 Subaccount Management Page – Edit User Link

| Field Name | Data Type | Length | Required | Default Value | Location | Comments |
|---|---|---|---|---|---|---|
| Password | AN | 20 | Yes* See Comment | Yes* See note following table | Page 2 | Concealed; to change, click on "Password" hyperlink to display Change Password Page (Sec. A.5.6) |
| E-mail | AN | See Comment | Yes | Yes | Page 2 | Must match form of a valid e-mail address |
| Contact Street Address 1 | AN | 40 | No | Yes | Page 2 | |
| Contact Street Address 2 | AN | 40 | No | Yes | Page 2 | |
| Contact City | AN | 30 | No | Yes | Page 2 | |
| Contact State/Province | A | N/A | No | Yes | Page 2 | No more than one from drop-down list of U.S. states, District of Columbia, Canada provinces and territories |
| Contact Zip/Postal Code | AN | 10 [1-6] [7-10] | No | Yes | Page 2 | If U.S., "xxxxx"("xxxx"). If Canada, "xnxnxn" |
| Contact Phone | N | 10 [1-3] [4-6] [7-10] | No | Yes | Page 2 | Three-digit area code and seven-digit phone number (no punctuation marks) |
| Contact Fax | N | 10 [1-3] [4-6] [7-10] | No | Yes | Page 2 | Three-digit area code and seven-digit phone number (no punctuation marks) |

## Table A.14 Subaccount Management Page – Edit User Link (continued)

| Field Name | Data Type | Length | Required | Default Value | Location | Comments |
|---|---|---|---|---|---|---|
| Permissions | Array | N/A | No | Yes | Page 2 | 0–6 check boxes including:<br>– "IFTA Access"<br>– "RPC Access"<br>– "IRP Access"<br>– "OSOW Access"<br>– "Edit Profile"<br>– "View Carrier"<br>Checks cannot exceed permissions held by the master account |

Note: *Yes indicates that a default value may be drawn from the $\text{PORTAL}_{\text{CS}}$ profile of the user.

## Table A.15 Subaccount Management Page – Add User Option

| Field Name | Data Type | Length | Required | Default Value | Location | Comments |
|---|---|---|---|---|---|---|
| Username | AN | 20 | Yes | No | Page 2 | Minimum of six characters, including alphanumeric, underscore, hyphen, and period |
| Password | AN | 20 | Yes | No | Page 2 | Minimum of six characters, including alphanumeric, underscore, hyphen, and period |
| Confirm Password | AN | 20 | Yes | No | Page 2 | Value must equal "Password" |
| E-mail | AN | See Comment | Yes | No | Page 2 | Must match form of a valid e-mail address |
| Contact Street Address 1 | AN | 40 | No | No | Page 2 | |
| Contact Street Address 2 | AN | 40 | No | No | Page 2 | |
| Contact City | AN | 30 | No | No | Page 2 | |
| Contact State/Province | A | N/A | No | No | Page 2 | No more than one from drop-down list of U.S. states, District of Columbia, Canada provinces and territories |
| Contact Zip/Postal Code | AN | 10<br>[1-6]<br>[7-10] | No | No | Page 2 | If U.S., "xxxxx"("xxxx"). If Canada, "xnxnxn" |

**Table A.15 Subaccount Management Page – Add User Option (continued)**

| Field Name | Data Type | Length | Required | Default Value | Location | Comments |
|---|---|---|---|---|---|---|
| Contact Phone | N | 10<br>[1-3]<br>[4-6]<br>[7-10] | No | No | Page 2 | Three-digit area code and seven-digit phone number (no punctuation marks) |
| Contact Fax | N | 10<br>[1-3]<br>[4-6]<br>[7-10] | No | No | Page 2 | Three-digit area code and seven-digit phone number (no punctuation marks) |
| Permissions | Array | N/A | No | No | Page 2 | 0–6 check boxes are displayed that correspond to permissions held by the master account, from among:<br>– “IFTA Access”<br>– “RPC Access”<br>– “IRP Access”<br>– “OSOW Access”<br>– “Edit Profile”<br>– “View Carrier” |

## A.6 Security Design

Security for the CVISN/PRISM systems will occur at two levels, physical and logical. Physical security of the system will include protection of the systems from theft and natural disasters. Logical security will ensure the integrity of the system applications and data. DOIT will play a primary role in both levels of security, as noted below:

### A.6.1 Physical Security

DOIT will house all the CVISN/PRISM systems at its secured data center located in East Hartford, Connecticut. This location meets all state security requirements including secured access to the system hardware.

$\text{CVIEW}_{\text{CS}}$ and Database servers are dedicated wholly to CVISN/PRISM operations and will be located behind the State’s firewall. Remote access to $\text{CVIEW}_{\text{CS}}$ and database server will only be allowed to authorized users via a Nortel virtual private network. DOIT will provide one or more instances of the shared WebSphere servers to house the CVISN/PRISM web applications. DOIT is responsible for establishing security procedures for these WebSphere severs. Due to the shared nature of the WebSphere servers, no remote access will be allowed.

A variety of network connections are included within the CVISN/PRISM Release 1 functionality. In case of connections within the State firewall, security is assured due to the fact that these connections reside entirely behind state firewalls. In case of connections between a state system and a non-state system, the connections cross the state firewall. Hence, it is the responsibility of the two parties involved to make sure that the connection is secure. Depending on the type of connection, it may be conducted "in the clear" or be encrypted.

### A.6.2 Logical Security

Logical security occurs at three levels – application security, data security and data element security.

- **Application Security:** Communication between the web applications and the users is conducted using https (secure hypertext transfer protocol) ensuring security. A valid account is required in order to log onto the system. By default, web sessions within $\text{PORTAL}_{\text{CS}}$ will time out after four hours without activity. Once a time out occurs, the user will be required to supply their username and password prior to the next operation. For users that access the Connecticut CVISN/PRISM web systems from public terminals, e.g., from public libraries or Internet kiosks, a checkbox will be provided on the login page. This checkbox will read "I am using a public computer." If this box is checked, the timeout will be changed to 10 minutes as part of the login process. This provides the user with some control over the timeout period as well as additional security to prevent unauthorized users from accessing accounts left unattended in public locations. The timeout process will extend to the $\text{IFTA}_{\text{CS}}$ credential web application. Timeouts in the MVS/Express, e-PASS and RPC web applications will be handled separately according to the rules used in these systems.

- **Data Security:** Access to the $\text{CVIEW}_{\text{CS}}$ database will be controlled using Oracle security with no user or system being granted greater access than necessary. Individuals may receive accounts to directly access the CVISN/PRISM database. These accounts may be used to examine or change CVISN/PRISM data. Currently no one has been identified by the State to receive this type of access. For a person to have this level of access, he/she must be authorized by the State, be conversant with Oracle and thoroughly understand the CVISN/PRISM process. Only the $\text{CVIEW}_{\text{CS}}$ program and LSIs will have write access to the $\text{CVIEW}_{\text{CS}}$ and CVIEWLSI schemas within the CVIEW database. Other users and systems, including the $\text{PORTAL}_{\text{CS}}$, IFTA, and OSOW applications, will use read-only accounts that expose only the minimum data necessary to perform their functions.

  The CVISN/PRISM Project Team will assign technical staff to administer the access rights and privileges to data. The assigned technical staff will coordinate with

Cambridge Systematics to establish the initial administrative rules of access for DMV, DRS and DOT data, respectively, including the prohibition of any non-DMV, non-DRS or non-DOT administrators to modify the rules of access for the respective agency data. The specific rules of agencies for data composition and access cannot be superseded. Any "super user" administrative authority to modify existing, agency defined, access rights and privileges will only be allowed after proper consideration and formal authorization is granted by the respective agency that owns the data.

- **Data Element Security:** This level of security is governed by two sets of rules: authoritative source rules and user access rules. Authoritative source rules apply only to data received and processed by the $\text{CVIEW}_{\text{CS}}$ program and ensure that organizations only update those elements for which they can provide reliable data. When two different systems can supply the same information, these constraints also ensure that the values from the most authoritative system are retained. User access rules apply only to data sent by the $\text{CVIEW}_{\text{CS}}$ program in response to a subscription fulfillment and can be used to adjust outgoing data to conform to privacy regulations. These rules list which data items can be delivered to each user. They are applied by the $\text{CVIEW}_{\text{CS}}$ output message handler prior to sending any information to a subscription user. At present, the only subscriptions identified for $\text{CVIEW}_{\text{CS}}$ in Connecticut are those necessary to transfer data to Model MACS and SAFER.

### A.6.3 Back-ups

DOIT will be responsible for conducting regular backups of all data stored in the CVISN/PRISM systems housed at its data center. These backups will be conducted in accordance with DOIT policy and standards. DOIT also will be responsible for determining the backup schedule; although a complete backup of the production Oracle databases should take place at least daily. It is recommended that DOIT maintain a redundant set of backups for all databases should one backup media become corrupted. It should be noted that the project's staging servers are not designed to serve as data backups in case of a disaster. The databases on the staging servers only will be populated at the outset of the project. These databases will be allowed to age and will not be updated.

### A.6.4 Recovery

DOIT will be responsible for restoring the CVISN/PRISM systems should a catastrophic failure occur. Recovery will take place in accordance with DOIT policies and standards. The timeliness of the recovery will be established in the service agreement between DOIT and DMV. At a minimum, the system should be recovered to the last complete backup on file.

## A.7 User Self-Registration

PORTAL$_{CS}$ will support self-registration of carriers and service bureaus. When a user arrives at the PORTAL$_{CS}$ login page they will be allowed to:

- Login using an existing account;
- Self-register as a carrier;
- Self-register as a service bureau; and
- Request that a forgotten password be reset.

The self-registration processes for carriers and service bureaus are similar. All users will be required to provide a username and password. The username must be unique in the PORTAL$_{CS}$ database of users. All users will be required to provide a company name; an FEIN/SSN, which also must be unique in the database of users; and address information, including an electronic mail address. Users will be able to enter additional addresses and provide contact information. Carriers will be asked to provide more information than service bureaus because individual carriers will have unique identifiers (e.g., U.S. DOT number, IRP Account Number, IFTA Account Number and Tax Registration Number) that do not apply to a service bureau. These values will be optional because they may not exist for all users.

The self-registration process creates a master account. The master account is the main account for a carrier or service bureau. The master account can maintain the business-level information, e.g., FEIN and business address for the carrier, as well as create and maintain subaccounts associated with the master account. Subaccounts provide additional users within a company access to PORTAL$_{CS}$ in order to perform some or all of the functions available to the master account. The master account holder will be responsible for determining/updating the functions that a subaccount user will be allowed to perform. Subaccounts always inherit the business-level information associated with the master account and cannot change this information.

During the self-registration process, PORTAL$_{CS}$ sets default values for access to functions that a user may perform. These default values are based on business logic provided by the State and vary based on whether the user is a carrier or a service bureau. The default values for all credentials are outlined in Section A.9.

Once a user has successfully registered, they may log into the PORTAL$_{CS}$ by providing their username and password on the PORTAL$_{CS}$ login screen. If this username and password match entries in the PORTAL$_{CS}$ database of users, the user will be directed to the PORTAL$_{CS}$ main menu.

# A.8 State Account Creation

During Release 1, State user accounts will be created manually by Cambridge Systematics. State users will not have access to the web-based credentialing applications and instead will use in-state systems to perform these functions. The CVISN/PRISM Project Team will assign technical staff to administer the access rights and privileges to data. The assigned technical staff will coordinate with CS to establish the initial administrative rules of access to DMV, DRS and DOT data, respectively, including the prohibition of any non-DMV, non-DRS, or non-DOT administrators to modify the rules of access for the respective agency data. The specific rules of agencies for data composition and access cannot be superseded. Any "super user" administrative authority to modify existing, agency-defined access rights and privileges only will be allowed after proper consideration and formal authorization is granted by the respective agency that owns the data.

# A.9 Account Management

## A.9.1 Account Maintenance

The "Edit My Account" link on the portal main menu will be enabled only if the Maintain Account flag is set to Y for the current user in the $\text{PORTAL}_{\text{CS}}$ database of users. Clicking this hyperlink will transfer the user to a page where current registration information for the account is displayed. All information associated with the account may be changed except the username and the FEIN/SSN.

A separate hyperlink is provided for changing the password. The user must supply the current password as well as the new password in order to complete the change.

## A.9.2 Subaccount Maintenance

The "Manage User Accounts" link on the portal main menu will be enabled only if the Maintain Subaccounts flag is set to Y for the current user in the $\text{PORTAL}_{\text{CS}}$ database of users. Clicking this hyperlink will transfer the user to a page displaying the current list of subaccounts.

The subaccount list window will include an Add User button. Clicking this will transfer the user to the subaccount entry window. The subaccount entry window is similar to the self-registration window. However, business-level information cannot be entered or changed on this page. Personal information must be entered for the subaccount, including a unique username, a password and an e-mail address. Contact information unique to the subaccount also may be entered.

Permissions also may be assigned to the subaccount. Only permissions that are available to the master account may be granted to the subaccount. For example, if the master account has no access to the IRP web application then the master account cannot assign this privilege to the subaccount. The following flags cannot be set for a subaccount because they are reserved for master accounts: Master Account and Maintain Subaccounts.

Information associated with existing subaccounts, including the permissions for that account, can be changed using the master account. On the subaccount list window, an Edit hyperlink will appear next to each subaccount. Clicking this hyperlink will bring up the subaccount entry window with the current information for the subaccount already displayed.

This information for the subaccount can be changed and updated. Subaccounts are enabled by default when created. The master account may disable or enable a subaccount from the subaccount list window. The Enabled checkbox next to a subaccount may be unchecked to disable the subaccount or checked to enable the subaccount. An Update button will apply the changes.

## A.10 State-Granted Credentialing Permissions

A flag will be set in the $PORTAL_{CS}$ database of users indicating that an account represents a carrier or service bureau. This flag exists at the business level and applies to all accounts for this business. Web-based credentialing systems may need to perform different operations for service bureaus than for carriers. In addition, when an account is created through the self-registration process, flags granting access to portal functionality will be set based on business rules specified by the individual Connecticut CVISN/PRISM agencies. The following flags will be set:

- **Enabled = Y.** All accounts are enabled by default. State personnel may disable accounts, in which case logins by this account will be denied. An interface to access this value will be provided in Release 2. Until that time, Cambridge Systematics, upon receiving a request from the State, will update this value.

- **Master Account = Y.** Accounts created through self-registration are master accounts. Subaccounts are created from within a master account using an option on the main portal menu.

- **Maintain Account = Y.** By default, master accounts can maintain their own information. Master accounts can maintain all the information associated with the master account, including addresses and identifiers like U.S. DOT number, which exist at the business level, as well as contact information associated with the master account. Subaccounts can maintain only information that is unique to the subaccount, e.g., contact information.

- **Maintain Subaccounts = Y for master accounts and N for subaccounts.** By default, master accounts can create, maintain and disable subaccounts associated with the master account.

- **View Carrier Information = N for carriers and N for service bureaus**. By default, carriers and service bureaus are prevented from viewing snapshot information. Access to view snapshot information must be granted explicitly by the State upon agreement from all CVISN/PRISM agencies. An interface to access this value will be provided in Release 2. Until that time, Cambridge Systematics, upon receiving a request from the State, will update this value. Carriers may be granted access to view their own carrier and vehicle snapshots. Service bureaus will not be granted access to view snapshots.

- **Access IFTA = Y.** By default, the Department of Revenue Services will allow access to the $\text{IFTA}_{\text{CS}}$ credential web application.

- **Access IRP = N.** By default, the Department of Motor Vehicles will not allow access to the MVS/Express web application. Access must be granted explicitly by DMV personnel. An interface to access this value will be provided in Release 2. Until that time, Cambridge Systematics, upon receiving a request from the State, will update this value.

- **Access OS/OW = Y.** By default, the Department of Transportation will allow access to the e-PASS web application. DOT will utilize an "opt-in, selective out" process for access to the e-PASS web application. An interface to access this value will be provided in Release 2. Until that time, Cambridge Systematics, upon receiving a request from the State, will update this value.

- **Access RPC = Y.** By default, the Department of Revenue Services will allow access to the New York Regional Processing Center's tax filing web application. The RPC may impose additional constraints on access to this application that are beyond the scope of this document.

## A.11 Interface to Credit Card Processing

As described in the CI/CVIEW Logical (General) System Design, Cambridge Systematics will create an interface that conforms with the PayFlow Pro Developer's Guide from VeriSign, Inc. 00000013/Rev. 2.

Cambridge Systematics will provide two web-based interfaces for credit card processing. The first will be a visual interface where the user will enter credit card information. The second will be a non-visual interface for use by backend systems that capture payment information using their own mechanism.

At the present time, no systems available as part of the initial Release 1 software plan to use either the visual or the non-visual credit card processing interfaces.

### *Visual Interface*

The visual credit card interface will consist of a single web page. State CVISN web-based credentialing systems wishing to collect payment via credit card will transfer control to this page passing an XML document containing the following information:

- Name of state agency – Possible values are “Department of Motor Vehicles,” “Department of Revenue Services” and “Department of Transportation”;
- Description of credential to be purchased;
- Name of current user and login sequence in the $\text{PORTAL}_{\text{CS}}$ database of users – These values will be provided to the credentialing system as part of the handoff from $\text{PORTAL}_{\text{CS}}$;
- Name of carrier for whom the credential is being purchased;
- Total amount due;
- Sales Tax due – This amount should be included in the Total Amount due and usually will be zero;
- Two invoice numbers, reference numbers or other values for this transaction in the backend system – The backend system will use these values to associate the result of the credit card operation with the original transaction; and
- URL to which the credit card result should be sent.

Prior to transferring control to the credit card interface, it will be the responsibility of the credentialing system to calculate all fees and present the user with a visual invoice. Printing of this invoice also is the responsibility of the credentialing system.

The following format will be used to transfer control to the visual interface:


```
<?xml version="1.0" encoding="UTF-8" ?>
<veriSignPaymentVO>
  <agencyName>Department of Revenue Services</agencyName>
  <credentialDescription>IFTA additional decals</credentialDescription>
  <carrierName>Cambridge Systematics, Inc.</carrierName>
  <loginSequence>10615</loginSequence>
  <username>TESTCARRIER</username>
  <invoiceNumber1>11111</invoiceNumber1>
  <invoiceNumber2>11111111111</invoiceNumber2>
  <totalAmount>30.0</totalAmount>
  <salesTax>0.0</salesTax>
  <returnURL>newApplication.do?fileApplicationAction=CreditCardReceipt</re
turnURL>
  <referenceNumber/>
  <resultCode/>
  <resultMessage/>
  </veriSignPaymentVO>
```

The following format will be used to return control from the visual interface:


```
<?xml version="1.0" encoding="UTF-8" ?>
<veriSignPaymentVO>
  <agencyName>Department of Revenue Services</agencyName>
  <credentialDescription>IFTA additional decals</credentialDescription>
  <carrierName>Cambridge Systematics, Inc.</carrierName>
  <loginSequence>10615</loginSequence>
  <username>TESTCARRIER</username>
  <invoiceNumber1>11111</invoiceNumber1>
  <invoiceNumber2>11111111111</invoiceNumber2>
  <totalAmount>30.0</totalAmount>
  <salesTax>0.0</salesTax>
  <returnURL>newApplication.do?fileApplicationAction=CreditCardReceipt</returnURL>
  <referenceNumber>V64A31384076</referenceNumber>
  <resultCode>0</resultCode>
  <resultMessage>Approved&AUTHCODE</resultMessage>
</veriSignPaymentVO>
```


The visual interface web page will include the name of the state agency, the credential description, the carrier name and the amount due. It will prompt for the following information:

- Credit card type (VISA or MasterCard only) – Required;
- Credit card account number – Required;
- The street address (number and street name) and zip code of the credit card account holder – Required;
- The CVV2 validation code on the credit card – Required;
- The credit card expiration date (must be greater than or equal to the current month and year) – Required; and
- Customer Code – Applicable to purchasing cards only.

The information supplied by the user will be combined with the total amount due, name of the current user, the reference number and other values as necessary to create a valid credit card transaction.

Fixed values included in these transactions will be tied to the merchant account established by that agency. If an agency should determine that more than one merchant account is required for electronic credit card transactions processed by this page, then any fixed values required as part of the transaction must be supplied by the credentialing system as part of the original data transmission.

The credit card transaction will be submitted to the VeriSign API. The State must supply the appropriate VeriSign software installed on the web application server as well as the connections necessary to reach the Global Payments financial network.

Following the call to the VeriSign API, the Cambridge Systematics page immediately will transfer control back to the credentialing system. Cambridge Systematics will use the URL included in the original data transmission. All information included in the original data transmission will be returned to the credentialing system as well as the following items:

- Reference number – Provided by VeriSign;
- Result code – 0 indicates the transaction was approved, a value less than 0 indicates a communication error – in this case no transaction was attempted, a value greater than 0 indicates a decline or error; and
- Result message – This string will include a message associated with the result code.

Table A.16 contains a complete list of system-oriented result codes. Table A.17 contains a complete list of transaction-oriented result codes.

## Table A.16 Result Codes – System Errors

| Result | Description |
|---|---|
| -1 | Failed to connect to host |
| -2 | Failed to resolve hostname |
| -5 | Failed to initialize SSL context |
| -6 | Parameter list format error: & in name |
| -7 | Parameter list format error: invalid [ ] name length clause |
| -8 | SSL failed to connect to host |
| -9 | SSL read failed |
| -10 | SSL write failed |
| -11 | Proxy authorization failed |
| -12 | Timeout waiting for response |
| -13 | Select failure |
| -14 | Too many connections |
| -15 | Failed to set socket options |
| -20 | Proxy read failed |
| -21 | Proxy write failed |
| -22 | Failed to initialize SSL certificate |
| -23 | Host address not specified |
| -24 | Invalid transaction type |
| -25 | Failed to create a socket |
| -26 | Failed to initialize socket layer |

## Table A.16 Result Codes – System Errors (continued)

| Result | Description |
|---|---|
| -27 | Parameter list format error: invalid [ ] name length clause |
| -28 | Parameter list format error: name |
| -29 | Failed to initialize SSL connection |
| -30 | Invalid timeout value |
| -31 | The certificate chain did not validate, no local certificate found |
| -32 | The certificate chain did not validate, common name did not match URL |
| -99 | Out of memory |
| -999 | User canceled payment operation |

## Table A.17 Result Codes – Transaction Errors

| Result | Description |
|---|---|
| 0 | Approved |
| 1 | User authentication failed |
| 2 | Invalid tender type. Your merchant bank account does not support the following credit card type that was submitted. |
| 3 | Invalid transaction type. Transaction type is not appropriate for this transaction. For example, you cannot credit an authorization-only transaction. |
| 4 | Invalid amount format |
| 5 | Invalid merchant information. Processor does not recognize your merchant account information. Contact your bank account acquirer to resolve this problem. |
| 7 | Field format error. Invalid information entered. See RESPMSG. |
| 8 | Not a transaction server |
| 9 | Too many parameters or invalid stream |
| 10 | Too many line items |
| 11 | Client time-out waiting for response |
| 12 | Declined. Check the credit card number and transaction information to make sure they were entered correctly. If this does not resolve the problem, have the customer call the credit card issuer to resolve. |
| 13 | Referral. Transaction was declined but could be approved with a verbal authorization from the bank that issued the card. Submit a manual Voice Authorization transaction and enter the verbal auth code. |
| 19 | Original transaction ID not found. The transaction ID you entered for this transaction is not valid. See RESPMSG. |
| 20 | Cannot find the customer reference number |

## Table A.17 Result Codes – Transaction Errors (continued)

| Result | Description |
|---|---|
| 22 | Invalid ABA number |
| 23 | Invalid account number. Check credit card number and resubmit. |
| 24 | Invalid expiration date. Check and resubmit. |
| 25 | Invalid Host Mapping. Transaction type not mapped to this host |
| 26 | Invalid vendor account |
| 27 | Insufficient partner permissions |
| 28 | Insufficient user permissions |
| 29 | Invalid XML document. This could be caused by an unrecognized XML tag or a bad XML format that cannot be parsed by the system. |
| 30 | Duplicate transaction |
| 31 | Error in adding the recurring profile |
| 32 | Error in modifying the recurring profile |
| 33 | Error in canceling the recurring profile |
| 34 | Error in forcing the recurring profile |
| 35 | Error in reactivating the recurring profile |
| 36 | OLTP Transaction failed |
| 50 | Insufficient funds available in account |
| 99 | General error. See RESPMSG. |
| 100 | Transaction type not supported by host |
| 101 | Time-out value too small |
| 102 | Processor not available |
| 103 | Error reading response from host |
| 104 | Timeout waiting for processor response. Try your transaction again. |
| 105 | Credit error. Make sure you have not already credited this transaction, or that this transaction ID is for a creditable transaction. (For example, you cannot credit an authorization.) |
| 106 | Host not available |
| 107 | Duplicate suppression time-out |
| 108 | Void error. See RESPMSG. Make sure the transaction ID entered has not already been voided. If not, then look at the Transaction Detail screen for this transaction to see if it has settled. (The Batch field is set to a number greater than zero if the transaction has been settled). If the transaction has already settled, your only recourse is a reversal (credit a payment or submit a payment for a credit). |
| 109 | Time-out waiting for host response |
| 111 | Capture error. Only authorization transactions can be captured. |
| 112 | Failed AVS check. Address and ZIP code do not match. An authorization may still exist on the cardholder's account. |
| 113 | Cannot exceed sales cap. For ACH transactions only. |
| 113 | Merchant sale total will exceed the cap with current transaction |

## Table A.17 Result Codes – Transaction Errors (continued)

| Result | Description |
|---|---|
| 114 | Card Security Code (CSC) Mismatch. An authorization may still exist on the card-holder's account. |
| 115 | System busy, try again later |
| 116 | VPS Internal error – Failed to lock terminal number |
| 117 | Failed merchant rule check. An attempt was made to submit a transaction that failed to meet the security settings specified on the VeriSign Manager Security Settings page. See VeriSign Manager User's Guide. |
| 118 | Invalid keywords found in string fields |
| 1000 | Generic host error. See RESPMSG. This is a generic message returned by your credit card processor. The message itself will contain more information describing the error. |

It will be the responsibility of the backend system to handle credit card transaction results, both successful and unsuccessful, based on business rules associated with the credential.

The visual interface also will allow the user to cancel the transaction without submitting credit card information. In this case, control will be transferred back to the credentialing system and the result code will equal -999 and the reference number will be blank. The credentialing system must handle this case as well.

All credit card transactions will be logged in the $PORTAL_{CS}$ database. All data provided by the credentialing system or returned by VeriSign will be logged. Data entered by the user, including credit card number, will not be stored.

### *Non-Visual Interface*

The non-visual credit card interface will consist of a single web page. State CVISN web-based credentialing systems that collect their own credit card payment information will transfer control to this page passing an XML document containing the following information:

- Name of state agency – Possible values are "Department of Motor Vehicles," "Department of Revenue Services" and "Department of Transportation";
- Description of credential to be purchased;
- Name of current user and login sequence in the $PORTAL_{CS}$ database of users – This value will be provided to the credentialing system as part of the handoff from $PORTAL_{CS}$;
- Name of carrier for whom the credential is being purchased;

- Total amount due;
- Sales Tax due – This amount should be included in the Total Amount due and usually will be zero;
- Two invoice numbers, reference numbers or other values for this transaction in the backend system – The backend system will use these values to associate the result of the credit card operation with the original transaction;
- URL to which the credit card result should be sent;
- Credit card type (VISA or MasterCard only) – Required;
- Credit card account number – Required;
- The street address (number and street name) and zip code of the credit card account holder – Required;
- The CVV2 validation code on the credit card – Required;
- The credit card expiration date (must be greater than or equal to the current month and year) – Required; and
- Customer Code – Applicable to purchasing cards only.

Prior to transferring control to the non-visual credit card interface, it will be the responsibility of the credentialing system to calculate all fees and, if appropriate, present the user with a visual invoice. Printing of this invoice also is the responsibility of the credentialing system.

The following format will be used to transfer control to the non-visual interface:


```
<?xml version="1.0" encoding="UTF-8" ?>
<veriSignPaymentVO>
  <agencyName>Department of Revenue Services</agencyName>
  <credentialDescription>IFTA additional decals</credentialDescription>
  <carrierName>Cambridge Systematics, Inc.</carrierName>
  <loginSequence>10615</loginSequence>
  <username>TESTCARRIER</username>
  <invoiceNumber1>11111</invoiceNumber1>
  <invoiceNumber2>11111111111</invoiceNumber2>
  <totalAmount>30.0</totalAmount>
  <salesTax>0.0</salesTax>
  <returnURL>newApplication.do?fileApplicationAction=CreditCardReceipt</returnURL>
  <creditCardType>MasterCard</creditCardType>
  <creditCardNumber>5555555555554444</creditCardNumber>
  <streetAddress>100 Main St., Apt #1A</streetAddress>
  <zip>022221111</zip>
  <validationCode>111</validationCode>
```

```
  <expirationDate>0407</expirationDate>
  <customerCode>111</customerCode>
  <referenceNumber/>
  <resultCode/>
  <resultMessage/>
</veriSignPaymentVO>
```


The following format will be used to return control from the non-visual interface:


```
<?xml version="1.0" encoding="UTF-8" ?>
<veriSignPaymentVO>
  <agencyName>Department of Revenue Services</agencyName>
  <credentialDescription>IFTA additional decals</credentialDescription>
  <carrierName>Cambridge Systematics, Inc.</carrierName>
  <loginSequence>10615</loginSequence>
  <username>TESTCARRIER</username>
  <invoiceNumber1>11111</invoiceNumber1>
  <invoiceNumber2>11111111111</invoiceNumber2>
  <totalAmount>30.0</totalAmount>
  <salesTax>0.0</salesTax>
  <returnURL>newApplication.do?fileApplicationAction=CreditCardReceipt</re
turnURL>
  <referenceNumber>V64A31384076</referenceNumber>
  <resultCode>0</resultCode>
  <resultMessage>Approved&AUTHCODE</resultMessage>
</veriSignPaymentVO>
```


The non-visual interface will function identically to the visual interface except there is no need to prompt the user for any information because all data items ordinarily supplied by the user are provided in the original data transmission. The non-visual interface will take this information and immediately format a transaction for the VeriSign API. This transaction will be submitted in a manner identical to the visual interface. The result of the transaction will be returned to the credentialing system in a manner identical to the visual interface. This result will not include any credit card information. Transaction logging for the non-visual interface will be identical to the visual interface.

The cancel operation is not valid for the non-visual interface.

### *Delayed Capture*

The State does intend to provide delayed capture functionality as a credit card payment option. Delayed Capture is a process by which authorization of a transaction (at credential entry time) is followed later by capture of the funds associated with the transaction (at credential approval time). This functionality will be included in interim Release 1.

### *Automated Clearing House (ACH)*

The State does intend to provide ACH capability for use by agencies. Credit card fees generally are based on a percentage of the transaction value and therefore are not suited to high-dollar-value transactions. At the present time, the State has not selected an ACH vendor. Cambridge Systematics and the State mutually have agreed to defer this functionality until such time as a vendor has been selected and complete technical details are available for the ACH interface. Cambridge Systematics has requested that the State provide ACH information by October 1, 2003 in order for ACH functionality to be included in interim Release 1.

## A.12 Error Handling

$PORTAL_{CS}$ is equipped with a series of error handling mechanisms. These mechanisms include:

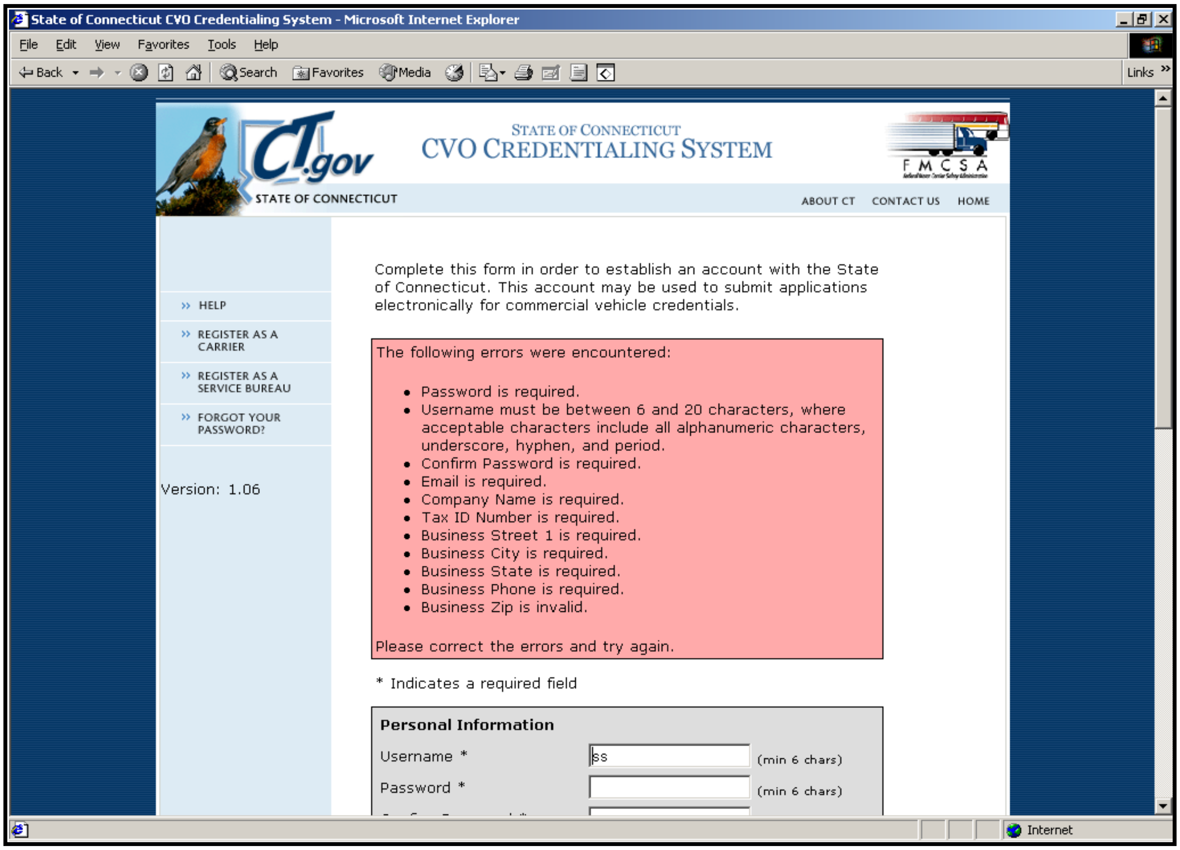
- Validation error messages;
- Error messages displayed to users; and
- Error logs.

Each of these error handling processes are described below.

### Validation Error Messages

Data entry fields in $PORTAL_{CS}$ are validated by the application for content and format. If a user's entry does not pass validation, a user is notified before his/her entries are processed. All validation error messages are presented at the top of the data entry screen in a red box following the phrase, "The following errors were encountered:". The error message identifies the data entry field(s) that must be corrected, as well as the proper content/format for the field. Users also are notified if they failed to enter a required field. Figure A.13 illustrates a potential validation error message on the Carrier Registration Page.

## Figure A.13 Sample Validation Error Message




## Error Messages Displayed to Users

PORTAL$_{CS}$ also contains a series of error messages that are presented if a user attempts an "illegal" operation (i.e., create a new account with a username that already exists in the system) or if the application experiences an error. Table A.18 summarizes all of the possible errors encountered in PORTALcs and the corresponding error message that will be displayed.

## Table A.18 PORTAL Error Messages

| Error Type | Error Message Displayed |
|---|---|
| Error connecting to the database | An error occurred due to a database failure. Please contact Technical Support for the CVO Credentialing System to report this problem. Technical Support information can be found by clicking on 'Contact Us.' Click on 'Home' to return to the main page. |
| Internal server error occurs | An error occurred. Please contact Technical Support for the CVO Credentialing System to report this problem. Technical Support information can be found by clicking on 'Contact Us.' Click on 'Home' to return to the main page.<br>The service you have requested is temporarily unavailable. Please try again later. If this problem persists, please contact Technical Support for the CVO Credentialing System to report this problem. Technical Support information can be found by clicking on 'Contact Us.' Click on 'Home' to return to the main page. |
| Error connecting to the email server | An error occurred while attempting to send email. Please contact Technical Support for the CVO Credentialing System to report this problem. Technical Support information can be found by clicking on 'Contact Us.' Click on 'Home' to return to the main page. |
| Attempt to create an account or subaccount with a duplicate username | The specified Username already exists in the system. |
| Attempting to create a new account with a Tex Registration ID associated with an existing account | The specified Tax ID already exists in the system. |
| User session expired | Your session has expired. Please login again. |
| Errors regarding query for a carrier and vehicle information | Carrier is not found. Please try again.<br>Program error: illegal query parameter.<br>Program error: no carrier found in session. |
| Error when Service Bureau selects a carrier with an inactive IFTA account. | This carrier is not active in the system. Please select a different carrier. |
| Error when FEIN/SSN found on IFTA Clearinghouse revoked list. | We're sorry. The FEIN or SSN you supplied cannot be processed through this system. Please submit form CT-IFTA-2 to the Connecticut Department of Revenue Services. |

## Error logs

PORTAL$_{CS}$ also produces two WebSphere logs that record errors in the operation of the application (i.e. a stale database connection). A system administrator can check these logs periodically to determine if PORTAL$_{CS}$ is performing as planned. The error logs are contained in the files:

- cvisn_app_stderr.txt; and
- cvisn_app_stdout.txt.

These files are stored at e:\WebSphere\appserver\logs on the staging server in Connecticut. Cambridge Systematics does not have access to the State's production server but will request a copy of the error log files from DOIT, if necessary.